Міністерство транспорту та зв'язку України
Міністерство освіти і науки України
Державний університет інформаційно-комунікаційних технологій

Інформаційна безпека систем електронного документообігу

(Укладач В.В. Богуш)

Київ 2007

ЗМІСТ

ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ

АД	- архіви документів
БД	- база даних
ДСК	- для службового користування
ЕД	- електронний документ
ЕП	- електронний підпис
ІТС	- інформаційно-телекомунікаційна система
КВД	- контроль виконавчої дисципліни
КЗЗ	- комплекс засобів захисту
КС	- комп’ютерна система
НД	- нормативний документ
НСД	- несанкціонований доступ
ОС	- операційна система
ПЗ	- програмне забезпечення
САД	- підсистема автоматизації діловодства
СЕД	- система електронного документообігу
СМД	- підсистема маршрутизації документів
ТЗІ	- технічний захист інформації
API	- Application Programming Interface
CAD	- Computer-Aided Design
CGI	- Common Gateway Interface
DMS	- Document Management Systems
ECM	- Enterprise Content Management
EDMS	- Electronic Document Management Systems
IDC	- Internet Database Connector
IIS	- Internet Information Server
IVP	- Integrity Verification Procedures
TP	- Transformation Procedures

ВСТУП

Процес управління і документообіг щільно пов'язані єдиною технологією реалізації функції управління. Метою документообігу являється забезпечення управлінської діяльності, процесу прийняття рішень цінною, корисною, своєчасною, повною та достовірною інформацією. Управлінню економічними, соціальними, політичними, виробничими структурами властива стабільність побудови і схожість документообігу.

Принципи і направлення руху традиційних та електронних документів в апараті управління єдині при будь яких системах обробки та зберігання документованої інформації. Змінюються методи роботи з документами, але технологічний взаємозв'язок документообігу з процесом управління зберігається. Це припущення надає об'єктивну можливість для наукового вирішення проблем електронного документообігу.

Як технологічний процес документообігу являє собою схему (сукупність маршрутів) руху людиночитаних (традиційних), машиночитаних і електронних документів по встановлених пунктах їхнього обліку, розгляду, виконання і збереження для виконання творчих, формально-логічних і технічних процедур і операцій. При цьому основною характеристикою руху документованої інформації є його технологічна комплексність, тобто з'єднання в єдину сукупність управлінських, діловодних і поштових задач. Документообіг відображає весь “життєвий цикл” документа — період його активного життя в управлінському процесі і період його досить пасивного архівного життя. Відбувається передача документованої інформації не тільки в просторі, але і в часі.

Проте електронний документообіг більше уразливий ніж його паперовий попередник: з файлу простіше зробити копію, внести в нього несанкціоновані зміни, виготовити фальшивий документ і т.ін. Маючи порівняно недороге обладнання, можна організувати атаки на канали зв'язку, на основі яких функціонує система електронного документообігу. Крім того, у документообіг організації може бути залучена велика кількість людей, за кожним з яких закріплений ряд виконуваних операцій і група документів, з якого він працює, тобто співробітники виступають у певній ролі щодо системи документообігу. У зловмисника (в основному внутрішнього) виникає багато можливостей для здійснення несанкціонованого доступу.

1 СИСТЕМА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ЯК ОБ'ЄКТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Загальні відомості про електронний документообіг

На початку " документообіг" був відображенням терміна "діловодство", добре формалізованого в традиційному управлінні. Тоді засоби автоматизації документообігу зводяться до комп'ютеризації традиційних завдань діловодства — до формування справ й обліку документів, що зберігаються в них, контролю, виконанню й формуванню звітності й т.ін. Подібного терміна, що однозначно відповідає "документообігу" в українському розумінні, у західному комп'ютерному словнику немає. У фахівців у галузі автоматизації бухгалтерського обліку, фінансової й складської діяльності під документообігом розуміється підсистема програми, що забезпечує генерацію "паперової" звітності (зведених відомостей, накладних, довідок й ін.) на основі даних, породжуваних у системі. Залежно від специфіки описуваного програмного забезпечення (ПЗ), що реалізує електронний документообіг, є три близьких аналоги:

1) DMS (Document Management Systems) — системи керування документами, у російськомовній літературі мають точний переклад — "архіви документів";

2) DocFlow — системи, або системи маршрутизації документів;

3) WorkFlow-системи — "системи автоматизації бізнес-процесів", або "системи підтримки управління".

Останнім часом з'явилися терміни, близькі до теми автоматизації документообігу, — Document Warehousing (сховища документів) і Knowledge Management (керування знаннями). Вони є подальшим розвитком систем документообігу й необхідні для структуризації й довгострокового зберігання великих масивів нагромаджених в організації документів, а також оптимального пошуку необхідної інформації на масиві різнорідних нагромаджених документів.

Прийняття Верховною радою України Закону "Про електронні документи та електронний документообіг" [4] надає можливість ввести ряд визначень, що є базовими в даній області.

Електронний документ (ЕД) - документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа (рисунок 1.1).

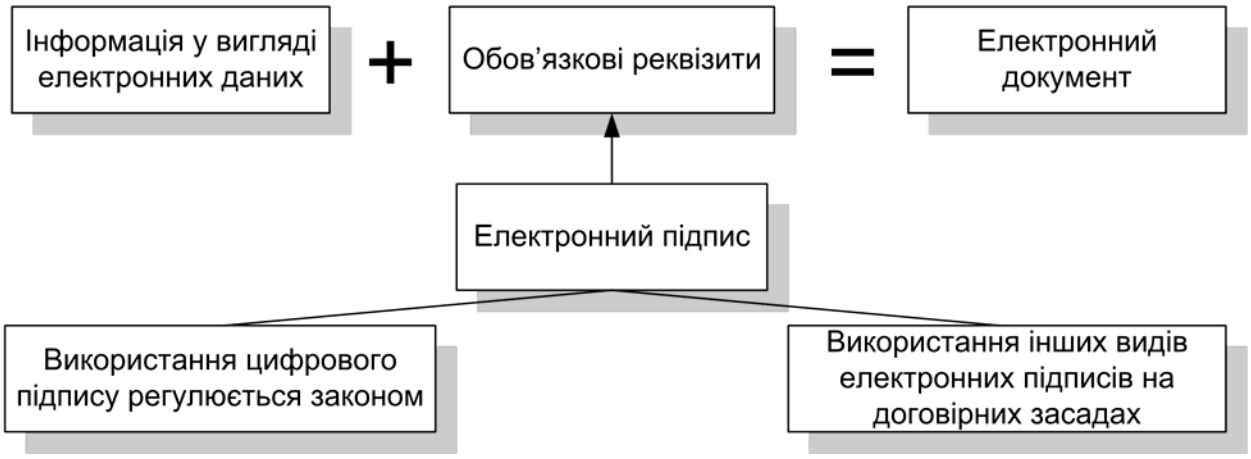

Рисунок1.1 – Структура електронного документу

Обов'язковий реквізит електронного документа – це обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили. Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Електронний підпис (ЕП) є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу. Автор електронного документа – це фізична або юридична особа, яка створила електронний документ [5].

Накладанням електронного підпису завершується створення електронного документа.

Відносини, пов'язані з використанням електронних цифрових підписів, регулюються законом.

Використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах.

Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним цифровим підписом автора (рисунок 1.2).

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

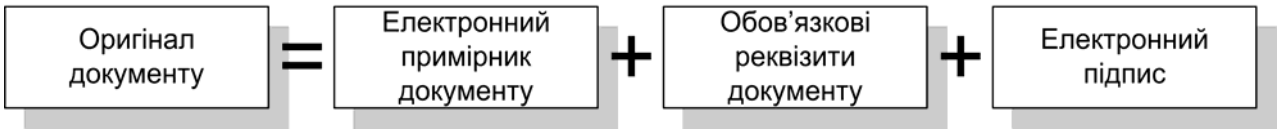

Рисунок 1.2 – Структура оригіналу електронного документу

Якщо автором створюються ідентичні за документованою інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу.

Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, втому числі у паперовій копії.

Електронна копія електронного документа засвідчується у порядку, встановленому законом.

Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством.

Електронний документ та його копії мають наступний правовий статус.

Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму.

Електронний документ не може бути застосовано як оригінал:

1) свідоцтва про право на спадщину;

2) документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів;

3) в інших випадках, передбачених законом.

Нотаріальне посвідчення цивільно-правової угоди, укладеної шляхом створення електронного документа (електронних документів), здійснюється у порядку, встановленому законом.

Електронний документообіг (обіг електронних документів) - сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів (рисунок 1.3).

Рисунок 1.3 – Електронний документообіг

Порядок електронного документообігу визначається державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством.

Відправлення та передавання електронних документів здійснюються автором або посередником в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ (рисунок 1.4).

Якщо автор і адресат у письмовій формі попередньо не домовилися про інше, датою і часом відправлення електронного документа вважаються дата і час, коли відправлення електронного документа не може бути скасовано особою, яка його відправила. У разі відправлення електронного документа шляхом пересилання його на електронному носії, на якому записано цей документ, датою і часом відправлення вважаються дата і час здавання його для пересилання.

Вимоги підтвердження факту одержання документа, встановлені законодавством у випадках відправлення документів рекомендованим листом або передавання їх під розписку, не поширюються на електронні документи. У таких випадках підтвердження факту одержання електронних документів здійснюється згідно з вимогами цього Закону.

Електронний документ вважається одержаним адресатом з часу надходження авторові повідомлення в електронній формі від адресата про одержання цього електронного документа автора, якщо інше не передбачено законодавством або попередньою домовленістю між суб'єктами електронного документообігу.

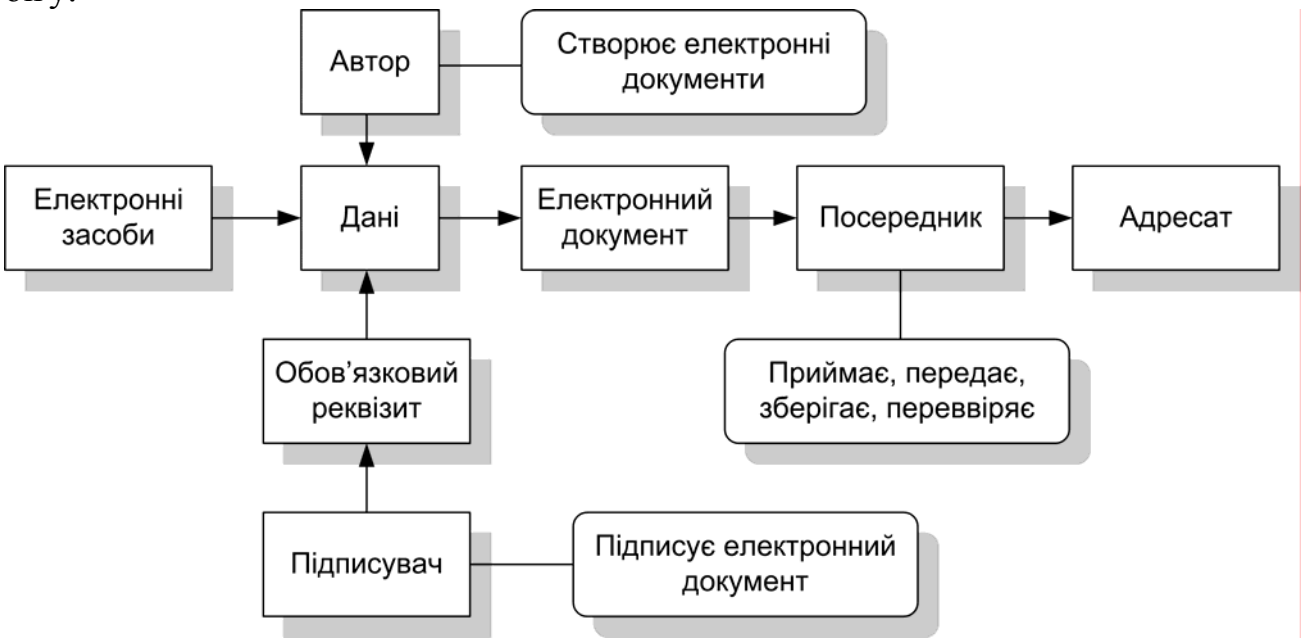

Рисунок 1.4 – Відправлення та передавання електронних документів

Якщо попередньою домовленістю між суб'єктами електронного документообігу не визначено порядок підтвердження факту одержання електронного документа, таке підтвердження може бути здійснено в будь-якому порядку автоматизованим чи іншим способом в електронній формі або у формі документа

на папері. Зазначене підтвердження повинно містити дані про факт і час одержання електронного документа та про відправника цього підтвердження.

У разі ненадходження до автора підтвердження про факт одержання цього електронного документа вважається, що електронний документ не одержано адресатом.

Якщо автор і адресат у письмовій формі попередньо не домовилися про інше, електронний документ вважається відправленим автором та одержаним адресатом за їх місцезнаходженням (для фізичних осіб - місцем проживання), у тому числі якщо інформаційна, телекомунікаційна, інформаційно-телекомунікаційна система, за допомогою якої одержано документ, знаходиться в іншому місці. Місцезнаходження (місцепроживання) сторін визначається відповідно до законодавства.

Перевірка цілісності електронного документа проводиться шляхом перевірки електронного цифрового підпису.

Суб'єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

Строк зберігання електронних документів на електронних носіях інформації повинен бути неменшим від строку, встановленого законодавством для відповідних документів на папері.

У разі неможливості зберігання електронних документів на електронних носіях інформації протягом строку, встановленого законодавством для відповідних документів на папері, суб'єкти електронного документообігу повинні вживати заходів щодо дублювання документів на кількох електронних носіях інформації та здійснювати їх періодичне копіювання відповідно до порядку обліку та копіювання документів, встановленого законодавством. Якщо неможливо виконати зазначені вимоги, електронні документи повинні зберігатися у вигляді копії документа на папері (уразі відсутності оригіналу цього документа на папері). При копіюванні електронного документа з електронного носія інформації обов'язково здійснюється перевірка цілісності даних на цьому носії.

При зберіганні електронних документів обов'язкове додержання таких вимог:

1) інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

2) має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний;

3) у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Суб'єкти електронного документообігу можуть забезпечувати додержання вимог щодо збереження електронних документів шляхом використання послуг посередника, у тому числі архівної установи, якщо така установа додержується вимог цієї статті. Створення архівів електронних документів, подання електронних документів до архівних установ України та їх зберігання в цих установах здійснюється у порядку, визначеному законодавством.

1.2 Типова система електронного документообігу

1.2.1. Призначення систем електронного документообігу

На думку аналітиків, електронний документообіг включає: створення документів, їхню обробку, передачу, зберігання, виведення інформації, що циркулює в організації або підприємстві, на основі використання комп'ютерних мереж [3]. Під керуванням електронним документообігом у загальному випадку прийнято розуміти організацію руху документів між підрозділами підприємства або організації, групами користувачів або окремих користувачів. При цьому, під рухом документів мається на увазі не їхнє фізичне переміщення, а передача прав на їхнє застосування з повідомленням конкретних користувачів і контролем за їхнім виконанням. IDC у такий спосіб визначає поняття система електронного документообігу (СЕД) (маючи на увазі EDMS – Electronic Document Management Systems): “СЕД забезпечують процес створення, керування доступом і поширення більших обсягів документів у комп'ютерних мережах, а також забезпечують контроль над потоками документів в організації. Часто ці документи зберігаються в спеціальних сховищах або в ієрархії файлової системи. Типи файлів, які, як правило, підтримують СЕД, включають: текстові документи, зображення, електронні таблиці, аудіодані, відеодані й Web-документи. До загальних можливостей СЕД ставляться: створення документів, керування доступом, конвертація даних і забезпечення безпеки даних”.

Головне призначення СЕД – це організація зберігання електронних документів, а також роботи з ними (зокрема, їхнього пошуку як по атрибутах, так і по вмісту). У СЕД повинні автоматично відслідковуватися зміни в документах, строки виконання документів, рух документів, а також контролюватися всієї їхньої версії й підверсії. Комплексна СЕД повинна охоплювати весь цикл діловодства підприємства або організації - від постановки завдання на створення документа до його списання в архів, забезпечувати централізоване зберігання документів у будь-яких форматах, у тому числі, складних композиційних документів. СЕД повинні поєднувати розрізнені потоки документів територіально вилучених підприємств у

єдину систему. Вони повинні забезпечувати гнучке керування документами як за допомогою твердого визначення маршрутів руху, так і шляхом вільної маршрутизації документів. У СЕД повинне бути реалізоване тверде розмежування доступу користувачів до різних документів залежно від їхньої компетенції, займаної посади й призначених їм повноважень. Крім того, СЕД повинна настроюватися на існуючу організаційно-штатну структуру й систему діловодства підприємства, а також інтегруватися з існуючими корпоративними системами.

Основними користувачами СЕД є великі державні організації, підприємства, банки, великі промислові підприємства й всі інші структури, чия діяльність супроводжується більшим обсягом створюваних, оброблюваних і збережених документів.

1.2.2 Основні властивості систем електронного документообігу

Відкритість

Всі СЕД побудовані за модульним принципом, а їхні API-інтерфейси є відкритими. Це дозволяє додавати до СЕД нові функції або вдосконалювати вже наявні. У цей час розробка додатків, інтегрованих із СЕД, стала окремим видом бізнесу в галузі промислового виробництва ПЗ, і безліч третіх фірм готові запропонувати свої послуги в даному сегменті ринку. Можливість щодо простого додавання до СЕД безлічі модулів від третіх фірм значно розширює їхні функціональні можливості. Наприклад, для СЕД розроблені модулі уведення документів зі сканера, зв'язку з електронною поштою, із програмами пересилання факсів й т.ін.

Високий ступінь інтеграції із прикладним ПЗ

Ключовою можливістю СЕД є високий ступінь їхньої інтеграції з різними програмними додатками за рахунок використання технологій OLE Automation, DDE, Active, ODMA, MAPI й т.ін. А безпосередньо при роботі з документами взагалі немає необхідності користуватися утилітами СЕД. Користувачі мають справу тільки зі звичайними прикладними програмами: у момент інсталяції клієнтської частини СЕД прикладні програми доповнюються новими функціями й елементами меню. Наприклад, користувач текстового процесора будь-який користувач, що бере участь у документообігу, може за своїм розсудом змінити існуючий маршрут проходження документів (або задати новий маршрут). При “твердій” маршрутизації маршрути проходження документів строго регламентовані, і користувачі не вправі їх міняти. Однак при “твердій” маршрутизації можуть оброблятися логічні операції, коли маршрут змінюється при виконанні яких-небудь заздалегідь заданих умов (наприклад, відправленню документа керівництву при перевищенні конкретним користувачем своїх посадових повноважень). У більшості СЕД модулів маршрутизації входить у комплект поставки, у деяких СЕД його необхідно здобувати окремо. Повнофункціональні модулі маршрутизації розробляють і поставляють треті фірми.

Розмежування доступу

У СЕД реалізовані надійні засоби розмежування повноважень і контролю за доступом до документів. У більшості випадків з їхньою допомогою визначаються наступні види доступу (набір повноважень, що задають, залежить від конкретної СЕД):

- повний контроль над документом;
- право редагувати, але не знищувати документ;
- право створювати нові версії документа, але не редагувати його;
- право анотувати документ, але не редагувати його й не створювати нові версії;

- право читати документ, але не редагувати його;
- право доступу до картки, але не до вмісту документа;
- повна відсутність прав доступу до документа (під час роботи із СЕД кожна дія користувача протоколюється, і, таким чином, вся історія його роботи з документами може бути легко проконтрольована).

Відстеження версій і підверсій документів

При одночасній роботі з документом відразу декількох користувачів (особливо, коли його необхідно погоджувати в різних інстанціях) дуже зручною функцією СЕД є використання версій і підверсій документа. Припустимо, виконавець створив першу версію документа й передав її на розгляд наступному користувачеві. Другий користувач змінив документ і створив на його основі вже нову версію. Потім він передав свою версію документа в наступну інстанцію третьому користувачеві, що створив уже третю версію. Через певний час, ознайомившись із зауваженнями й виправленнями, перший виконавець документа вирішує доробити вихідну версію й на її основі створює під-версію першої версії документа. Достоїнством СЕД є реалізована в них можливість автоматичного відстеження версій і подверсій документів (користувачі завжди можуть визначити, яка саме версія/підверсія документа є найбільш актуальною один по одному або часу їхнього створення).

Наявність утиліт перегляду документів різних форматів

До складу більшості СЕД входять утиліти для перегляду документів (так звані переглядачі - viewers), що розуміють багато десятків форматів файлів. З їхньою допомогою дуже зручно працювати, зокрема, із графічними файлами (наприклад, з файлами креслень у CAD-системах). Крім базового комплекту утиліт перегляду (що входить у кожну СЕД), у третіх фірм можна придбати додаткові утиліти, добре інтегрувальні із СЕД.

Анотування документів

При організації групової роботи над документами звичайно досить корисна можливість їхнього анотування. Тому що в деяких випадках користувачі позбавлені правий на внесення яких-небудь змін у документ у процесі його узгодження, то вони можуть скористатися з можливості його анотування. У більшості СЕД анотувань реалізується за рахунок включення в картку документа атрибута для анотації й передачі користувачам прав на редагування такого поля картки. Але таке рішення не завжди прийнятно (особливо при анотуванні графічного документа). У зв'язку із цим, у деяких СЕД існує так називана функція “червоного олівця”, за допомогою якої можна графічно вказати недоліки на самому зображенні. Програмні засоби, у яких реалізована функція «червоного олівця», широко пропонуються третіми фірмами.

Підтримка різних клієнтських програм

Клієнтами більшості СЕД можуть бути ПК із ОС MS Windows, Windows NT. У деяких СЕД використаються також платформи UNIX й Macintosh. Крім того, всі сучасні СЕД дозволяють працювати з документами через стандартні Web-навігатори. Тому що Web-навігатори можуть бути розміщені на різноманітних клієнтських платформах, те це полегшує рішення проблеми забезпечення роботи СЕД у гетерогенних мережних середовищах. При використанні Інтернет-технологій у СЕД з'являється ще один серверний компонент, відповідальний за доступ до документів через Web-навігатори.

1.2.3 Функціональна архітектура системи електронного документообігу

Система електронного документообігу (СЕД) — це корпоративна організаційно-технічна система, що представляє собою сукупність програмного, інформаційного й апаратного забезпечення, що реалізує електронний документообіг. Функціональна архітектура такої системи, що складається звичайно з ряду підсистем, може бути приблизно представлена так, як це показано на рисунку 1.5 [6].

Підсистема автоматизації діловодства (САД). У функції цього комплексу додатків не входить зберігання й переміщення документів, але входить фіксація документів у спеціальній базі даних (БД) із картками документів. Запис у БД характеризується набором значень атрибутів картки. Структура документів у БД опирається на так звану номенклатуру справ організації, а технологія їхнього обліку й обробки — на Положення про діловодство. Документи зберігаються в паперовому виді в спеціальному архіві, але в БД відображається їхнє поточне місце розташування й статус, включаючи атрибути контролю виконання. Розрізняють вхідні й вихідні документи, нормативно-розпорядницькі документи, документи колегіальних органів керування, довідкові документи й т.ін. Документи, що перебувають на контролі виконання, підрозділяються по виконавцях, статусу виконання, строкам виконання й ін. Крім обліку й пошуку документів у БД, система генерує звіти з відомостями виконання документів й іншою зведеною інформацією.

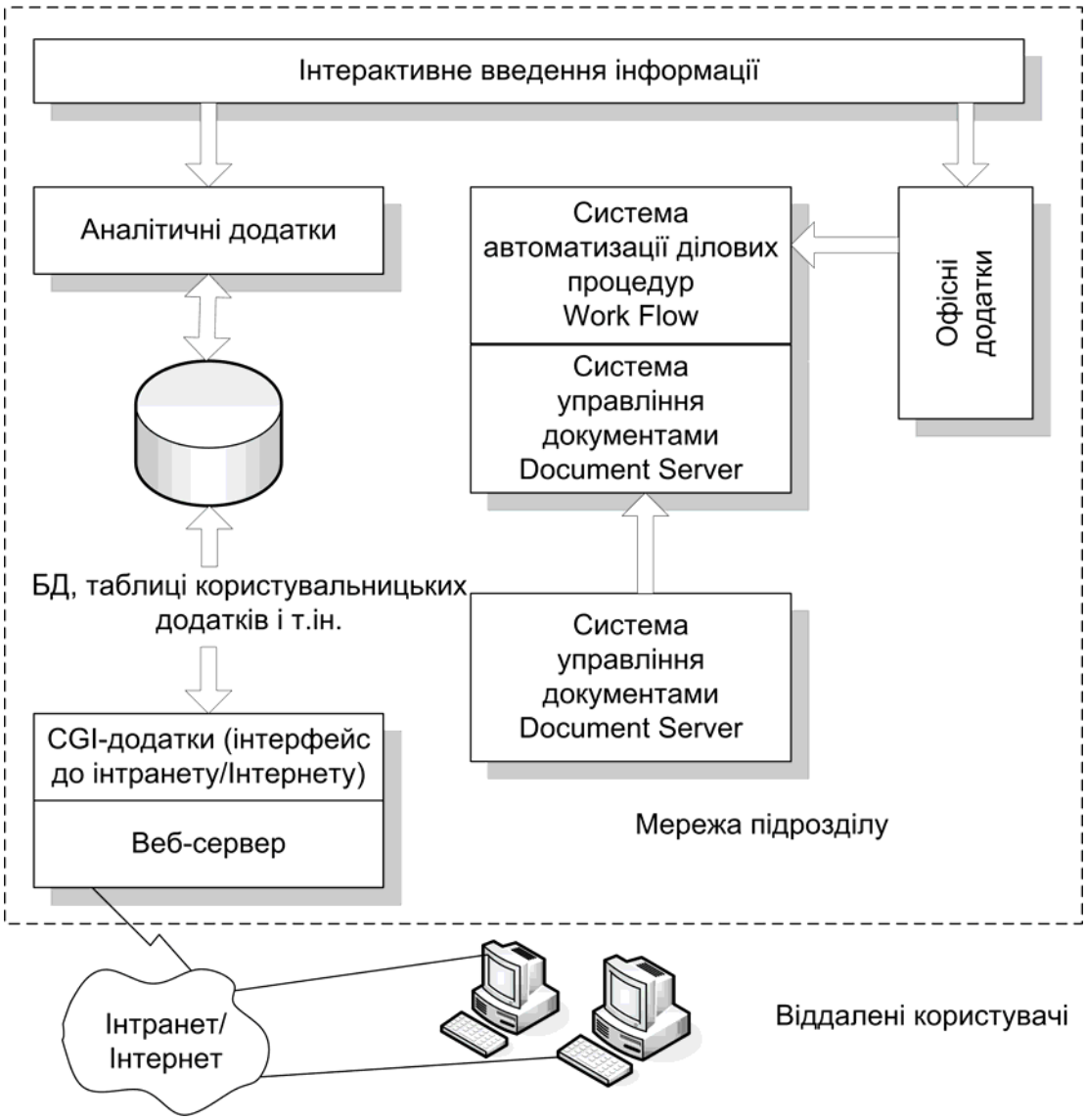

Рисунок 1.5 - Функціональна архітектура системи електронного документообігу

Підсистема "Архіви документів" (АД) зберігає або образ документа, або його зміст, або й те й інше. Вона забезпечує навігацію по ієрархії документів й їхній пошук. Якщо в САД пошук здійснюється по атрибутах документів, то в АД — повнотекстовий пошук по вмісту текстових фрагментів документа. Також, на відміну від САД, у АД зберігаються самі документи, для яких забезпечується розмежування прав доступу (на рівні користувачів, груп користувачів або ролей). Користувач ідентифікується мережним ім'ям або спеціальним ім'ям і паролем, певним у системі керування архівом. У АД забезпечується групова робота зі створюваними документами — це функція блокувань документів або Check-In/Check-Out-контроль (якщо один користувач починає редагувати документ, то він блокується для доступу інших до закінчення роботи). Підтримується контроль версій документів (або автоматично, або з ініціативи користувача). Якщо буде потреба користувач може повернутися до однієї з попередніх версій документа. Сервісними функціями АД є наступні: можливість створення резервних копій документів без припинення роботи системи, інтеграція із системами забезпечення оптимальної вартості зберігання даних й ін.

Підсистема введення документів і системи обробки образів документів. Під уведенням документів в архів розуміється їхнє переведення з паперового виду в електронний. У найпростішому випадку це зводиться до сканування. Але часто простого збереження образа документа недостатньо. Образ документа може зажадати так називаного анотування, накладення на образ документа додаткових образів, виділень, текстових позначок й ін. Також образ документа повинен бути вручну постачений набором атрибутів, що ідентифікують його в САД і АД. Більше складним завданням є автоматичне розпізнавання вмісту образа документа й формування документа, що містить його текст (використовується ПЗ розпізнавання тексту). Ще складніше розпізнавання вмісту форм. При цьому програма визначає наявність записів, у тому числі й рукописних, у певних полях бланка документа, розпізнає його вміст й автоматично заповнює значення атрибутів документа в системі. При необхідності значення певних полів бланка можуть вибиратися з певного в системі довідника.

Підсистема керування вартістю зберігання документів. При збереженні в архіві образів документів обсяги зберігання можуть швидко рости й досягати значних розмірів. При цьому інтенсивність звертання до документів нерівномірна і документи, що перебувають у роботі, потрібні часто; документи, робота з якими вже завершена, — рідко). Тому повинна забезпечуватися різна оперативність доступу до різних документів й автоматичне перенесення даних з більше “дорогих” пристроїв на більше “дешеві”. Тому що вартість зберігання документів в архіві, як правило, обернено пропорційна швидкості доступу, то можна скористатися відзначеною закономірністю для оптимізації вартості змісту архіву, що й робить дана система. Звичайно забезпечується робота з різними периферійними пристроями — накопичувачами на твердих магнітних дисках, On-line-оптичними стійками, нагромаджувачами на магнітній стрічці й CD-ROM-пристроями.

Підсистема маршрутизації документів (СМД) пересилає документи на робочі місця виконавців, збирає інформацію про поточний статус документів, здійснює консолідацію документів по завершенню роботи з ними на окремих етапах, забезпечує засобу доступу до інформації про поточний стан робіт з документами. СМД, як правило, містять засоби опису типових маршрутів проходження документів. На підставі розроблених маршрутних схем можуть породжуватися екземпляри бізнес-процесів роботи з документами (“тверда” маршрутизація). При “вільній” маршрутизації маршрут формується “стихійно” і кожен користувач системи з відповідними правами може визначити наступного виконавця документа. Адміністратор системи й менеджер конкретного бізнесу-процесу може контролювати поточний стан маршруту й вносити корективи. Можливі дві схеми маршрутизації документів — Offline й On-line. При першій відбувається фізичний витяг документа з АД й доставка його (наприклад, за допомогою електронної пошти) клієнтові. По завершенні роботи документ назад попадає в АД. Сама СМД є клієнтом АД й вносить відповідну інформацію в облікову БД. Друга схема не має на увазі фізичного переміщення документа — СМД забезпечує клієнтові інтерфейс для доступу до завдань на обробку документів.

Підсистема публікації інформації складається з веб-сервера й CGI-додатка, що реалізують зв'язок зі сховищами даних.

Підсистема комплексної автоматизації бізнес-процесів, або WorkFlow-система. На відміну від СМД об'єктом маршрутизації в них є сукупність даних, використовуваних у деякому бізнесі-процесі. Користувач одержує на робоче місце інформацію про те, що він повинен зробити, і всі необхідні для цього дані. WorkFlow-додаток визначає, яке додаток повинне бути запущене для реалізації функцій на даному робочому місці, і передає туди необхідні дані. Користувач виконує тільки необхідні функції, всю рутинну роботу (визначення послідовності дій, доставку необхідної інформації, контроль своєчасності виконання роботи й ін.) виконує система WorkFlow. Функції WorkFlow-додатків виходять за рамки функцій систем документообігу. Однак технології, використовувані в даних додатках, дуже близькі технологіям, використовуваним у СМД. До того ж маршрутизація документів може розглядатися як окремий випадок завдання побудови WorkFlow-системи.

Узагальнююча підсистема адміністрування й конфігурування СЕД може бути реалізована за допомогою: настроювання штатних засобів адміністрування операційної системи, на якій базується сервер; спеціалізованого додатка, що запускає з адміністраторськими правами й доступ, що має, до системних функцій операційної системи сервера БД; набору спеціальних процедур і функцій, доступ до яких можливий тільки за умови входу в систему із правами адміністратора.

1.2.4 Рівнева архітектура системи електронного документообігу

Рівнева архітектура системи представлена на рисунку 1.6.

У якості стандартного мережного протоколу найчастіше використовується протокол зі стека TCP/IP, що забезпечує як взаємодію робочих станцій в Microsoft Network, так і взаємодію з веб-сервером (інформаційно-телекомунікаційною системою). Формування документів, внесення й адміністрування нормативно-довідкової інформації, аналіз по окремих документах і напрямкам діяльності, статистичний аналіз діяльності підприємства в цілому й підготовка звітів реалізуються користувальницьким додатком на основі SQL-сервера, доступним із клієнтських робочих місць.

Як центральне сховище інформації може використатися, наприклад, СУБД MS SQL Server. У таблицях SQL зберігається вся інформація, необхідна для роботи DMS-сервера й аналітичного користувальницького додатка. Для організації публікації інформації можливе застосування Internet Information Server (IIS). Функції інтерактивного доступу до інформації з SQL-сервера виконує додаток у стандарті Common Gateway Interface (CGI-додаток).

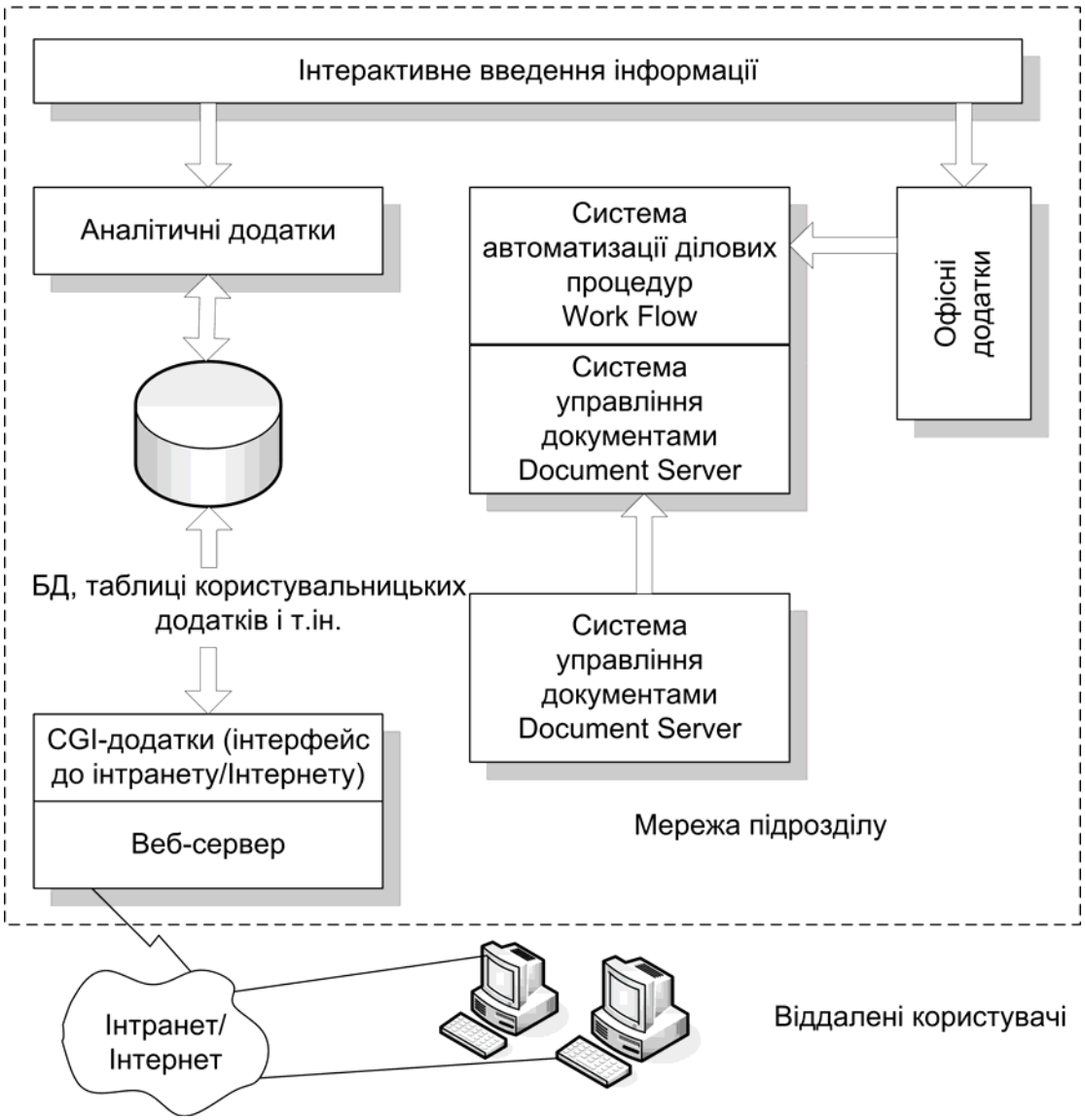

Рисунок 1.6 - Рівнева архітектура системи електронного документообігу

Адміністрування СЕД здійснюється стандартними засобами операційної системи. Про файли клієнтів зберігаються на сервері. Доступ клієнтів до сервера реалізується через стандартний веб-браузер. На кожній клієнтській станції встановлений пакет офісних додатків. Конфігурація клієнтів здійснюється адміністратором системи централізовано.

У наведеному модульному поділі системи пропущений модуль, відповідальний за захист інформації в процесі її зберігання й обробки. У захищеної СЕД підсистема безпеки може й не виділятися в окремий блок, тому що організація захисних механізмів невіддільна від реалізації конкретних функцій інших підсистем і часто не можна провести чіткий поділ на що захищають і відкриті ресурси системи. В істинно захищеній системі підсистема безпеки залишається прозорої для авторизованого користувача й непереборної для зломщика.

СЕД забезпечують процес створення, керування доступом і поширення більших обсягів документів у мережах, а також контроль над потоками документів в організації. Часто ці документи зберігаються в спеціальних сховищах або в ієрархії файлової системи. Типи файлів, які, як правило, підтримують СЕД,

включають текстові документи, образи, електронні таблиці, аудіо-, відеодані й документи Web. Загальними можливостями СЕД є створення документів, керування доступом, перетворення й безпека.

У СЕД реалізовані надійні засоби розмежування повноважень і контролю за доступом до документів. У більшості випадків з їхньою допомогою визначаються наступні види доступу (набір повноважень, що задають, залежить від конкретної СЕД):

- повний контроль над документом;
- право редагувати, але не знищувати документ;
- право створювати нові версії документа, але не редагувати його;
- право анотувати документ, але не редагувати його й не створювати нові версії;
- право читати документ, але не редагувати його;
- право доступу до картки, але не до вмісту документа;
- повна відсутність прав доступу до документа (під час роботи із СЕД кожна дія користувача протоколюється; тому вся історія його роботи з документами може бути легко проконтрольована).

Таким чином, СЕД повинні містити як функціональне ПЗ (для зберігання й обробки інформації, обміну даними), так і програмні або апаратно-програмні засоби захисту інформації (для шифрування, вироблення ЕП, захисту від НСД).

1.2.5 Технологія реалізації системи електронного документообігу

Найпоширенішою технологією реалізації СЕД є класична платформа клієнт-сервер з розподіленою моделлю зберігання даних, організацією колективного доступу до них й їхньої обробки. У системі, де серверним додатком є БД, сервер відповідає за створення й підтримку об'єктів БД, таких, як таблиці, індекси. Сервер підтримує цілісність дані бази і її безпеку. Крім того, він повинен забезпечувати можливість відновлення операцій у випадку виникнення різних збоїв.

Концепція ECM

Питання технології СЕД досить складний внаслідок швидкого розвитку ринку цих систем. Тим більше, що починаючи з 2001 р. все більшу популярність стала набирати концепція “керування корпоративним умістом (Enterprise Content Management – ECM)”, а не керування електронним документообігом (відповідно до “Forrester TechRankings”). Термін ECM з'явився з легкої руки торговельної асоціації AIIM International і накриває собою всі системи керування корпоративною інформацією.

У той же час, якщо Forrester Research визначає ECM, як інтегрований підхід до керування документами й Web-змістом, то для консалтингової компанії Doculabs керування корпоративним умістом ECM являє собою “категорію, що поєднує можливості систем керування корпоративними документами й систем

керування вмістом зі здатністю керування повним життєвим циклом корпоративного вмісту (при триваючому росту числа його типів)".

З погляду галузевих аналітиків, концепція ECM пропонує багато бізнес-переваг. ECM-система, що інтегрує всі контентно- і процесно-орієнтовані технології усередині підприємства, забезпечує загальну інфраструктуру для керування його документообігом, що мінімізує необхідність розгортання й підтримки безлічі технологій для реалізації різних бізнес-функцій. Суть даного підходу (його ще називають інфраструктурним) полягає в тому, що корпоративний вміст не повинне належати тільки одному додатку або системі. Він повинен бути доступним для безлічі додатків і вільно поширюватися між ними. Важливою властивістю ECM-інфраструктури (що включає відповідні додатки більшості вендорів (поставщиків) галузі) є її незалежність від єдиного універсального сховища вмісту. В ECM-інфраструктурі інтегрується безліч спеціалізованих (або успадкованих) депозитаріїв (відновлювачів) даних (навіть від конкуруючих вендорів), включаючи, у тому числі, сховища електронних документів про вироби, електронну пошту, сховища Web-змісту, файлові системи й навіть СУБД. Таким чином, ECM-інфраструктура забезпечує загальний шар інтеграції (або віртуализації) для кожного репозитарія даних (дозволяючи робити запити до них звідки завгодно по всьому підприємству), тим самим мінімізуючи необхідність інтеграції систем керування електронними документами й систем керування вмістом від безлічі вендорів. Крім того, за допомогою ECM-інфраструктури реалізуються такі сервіси керування корпоративним умістом, як персоналізація, контроль доступу, керування повноваженнями користувачів й ін. (що спрощує адміністрування й супровід ECM-систем.

Можливості ECM-систем можна розділити на кілька основних категорій:

Загальні функції керування вмістом, під якими розуміється здатність управляти безліччю електронних об'єктів (зображеннями, офісними документами, графіками, кресленнями, Web-змістом, електронною поштою, відео, аудіо й мультимедіа). ECM-система забезпечує репозитарій для всіх цих типів електронних об'єктів з різними бібліотечними сервісами (профілюванням умісту, функціями check-in/check-out, керуванням версіями, веденням хронології ревізій, забезпеченням безпеки доступу до документів й ін.), а також здатність управляти даними об'єктами протягом усього їхнього життєвого циклу.

Функції керування процесами, під якими розуміється здатність автоматизації й керування бізнес-процесами й потоками робіт.

Інтеграція з іншими ECM-системами, що припускає здатність інтеграції ECM-системи с зовнішніми ERP-системами, офісними додатками, сховищами вмісту, іншими СЕД. Інтеграція може бути виконана за допомогою різних підходів, включаючи використання об'єктно-орієнтованих інтерфейсів (таких, як EJB), конекторів, API-інтерфейсів, технології інтеграції корпоративних додатків EAI (Enterprise Application Integration) і ін.

Слід відзначити, що ECM існує дотепер тільки як концепція, і ECM-інфраструктура сьогодні у великій мірі являє собою тільки погляд на перспективи розвитку ринку СЕД. Наприклад, деякі галузеві вендори багато говорять про керування вмістом, однак свої системи вони фокусують тільки на керуванні

Web-змістом або офісними документами. Крім того, у них відсутні чіткі погляди на способи створення відкритої ECM-інфраструктури, що інтегрує спеціалізовані репозитарії по всьому підприємству. По оцінці аналітиків компанії Doculabs (що дослідили рішення провідних розроблювачів EDMS-систем), хоча вендори й визнають важливість концепції ECM, їм ще досить далеко до її повної реалізації у своїх системах.

Класифікація СЕД

На думку аналітиків IDC, у цей час існують наступні основні типи СЕД (при цьому деякі із СЕД можуть одночасно ставитися до декількох типів, тому що мають відповідними для них функціями) [3]:

СЕД, орієнтовані на бізнес-процеси (business-process EDM). Вони лежать в основі концепції ECM. Системи цього типу (EDMS) призначені для специфічних вертикальних і горизонтальних додатків (іноді вони мають і галузеве застосування). EDMS-системи забезпечують повний життєвий цикл роботи з документами, включаючи роботу з образами, керування записами й потоками робіт, керування вмістом й ін. EDMS-системи забезпечують зберігання й пошук 2-D документів в оригінальних форматах (зображень, CAD-файлів, електронних таблиць й ін.) с можливістю їхнього угруповання в папки. Існує думка деяких галузевих аналітиків, що (залежно від використовувані схеми індексації й додатків) даний документно-орієнтований підхід може забезпечити в ряді EDMS-систем до 80% функціональності PDM-системи при меншій вартості впровадження. Найбільш відомими розроблювачами EDMS-систем є компанії Documentum (система Documentum), FileNet (системи Panagon й Watermark), Hummingbird (система PC DOCS) і ін. Вендори, більше інших компаній, що одержали великі результати в керуванні вмістом (наприклад, компанії Documentum й FileNet), сфокусували свою діяльність на реалізації в СЕД таких функцій, як керування шаблонами, керування динамічними презентаціями й публікація Web-змісту. Слід відзначити, що при тім, що майже всі EDMS-системи забезпечують гарний рівень реалізації репозитаріїв і бібліотечних сервісів для керування електронним вмістом (наприклад, образами й офісними документами), кожна з них найбільш сильна у своїй області. Наприклад, у системах від компаній Open Text й iManage найбільше добре пророблене керування офісними документами. У свою чергу, системи від компаній Tower Technology, FileNet, IBM й Identitech особливо сильні в керуванні зображеннями виробів більшого обсягу.

Корпоративні СЕД (enterprise-centric EDM). Системи цього типу забезпечують корпоративну інфраструктуру (доступну всім корпоративним користувачам) для створення документів, колективної роботи над ними і їхньої публікації. Базові функції корпоративних СЕД аналогічні функціям СЕД, орієнтованим на бізнес-процеси. Як правило, корпоративні СЕД не орієнтовані на використання тільки в якійсь конкретній галузі або на рішення вузького завдання. Вони впроваджуються, як загальнокорпоративні технології. Розробкою й просуванням корпоративних СЕД займаються компанії Lotus (система

Domino.Doc), Novell (Novell GroupWise), Open Text (система LiveLink), Keyfile, Oracle (система Context), iManage й ін. Наприклад, система Open Text Livelink забезпечує колективну роботу над документами по проекті для зовнішніх і внутрішніх користувачів, проведення онлайнових дискусій, розподілене планування й маршрутизацію документів й ін.

Системи керування вмістом (content management systems). Системи даного типу забезпечують створення вмісту, доступ і керування вмістом, доставку вмісту (аж до рівня розділів документів й об'єктів для їх наступного повторного використання й компіляції). Доступність інформації не у вигляді документів, а у вигляді об'єктів меншого розміру полегшує процес обміну інформацією між додатками. Керування Web-вмістом вимагає наявності можливості керування об'єктами різного вмісту, які можуть бути включені в Web-презентацію (наприклад, HTML-сторінки й Web-графіку). Крім того, керування З вимагає наявності можливості створення презентаційних шаблонів, за допомогою яких здійснюються презентація динамічного вмісту і його персоналізація (заснована на перевагах користувачів, їхніх профілях й ін.). На світовому ринку відомі системи керування вмістом від компаній Adobe, Excalibur, BroadVision, Documentum, Stellent, Microsoft, Divine, Vignette й ін. Певний рівень керування Web-вмістом пропонують також компанії FileNet, Tower й Identitech. У свою чергу, компанія IBM реалізує функції по керуванню Web-вмістом на базі рішень від компаній Interwoven й Open Market (через партнерські відносини з ними), а компанія Tower інтегрувала своє ПЗ по керуванню електронними документами з рішеннями по керуванню Web-вмістом від компанії Stellent.

Системи керування інформацією (information management systems) – портали. Такі системи забезпечують агрегування інформації, керування інформацією і її доставкою через Internet/intranet/extranet. З їхньою допомогою реалізується можливість нагромадження (і застосування) досвіду в розподіленому корпоративному середовищі на основі використання бізнес-правил, контексту й метаданих. За допомогою порталів забезпечується також доступ через стандартний Web-навігатор до ряду додатків електронної комерції (звичайно, через інтерфейс ERP-системи). Прикладами порталів є системи Excalibur, Oracle Context, PC DOCS/Fulcrum, Verity, Lotus (Domino/Notes, K-Station).

Системи керування зображеннями/образами (imaging systems). С їхньою допомогою здійснюється конвертація відсканованої з паперових носіїв інформації в електронну форму (звичайно, у форматі TIFF). Дана технологія лежить в основі перекладу в електронну форму інформації із всіх успадкованих паперових документів і мікрофільмів. У число базових функцій стандартної системи обробки зображень входять: сканування, зберігання, ряд можливостей по пошуку зображень й ін.

Системи керування потоками робіт (workflow management systems). Системи даного типу призначені для забезпечення маршрутизації потоків робіт будь-якого типу (визначення шляхів маршрутизації файлів) у рамках корпоративних структурованих і неструктурованих бізнес-процесів. Вони використаються для підвищення ефективності й ступеня контрольованості корпоративних бізнес-процесів. Системи керування потоками робіт звичайно здобуваються, як

частина рішення (наприклад, EDMS-системи або PDM-системи). Тут можна відзначити таких розроблювачів, як компанії Lotus (системи Domino/Notes й Domino Workflow), Jetform, FileNet, Action Technologies, Staffware й ін. Гарний рівень керування потоками робіт забезпечують у своїх рішеннях також компанії FileNet, IBM (через інтеграцію з ПЗ MQ Series Workflow), Identitech, Tower (через інтеграцію з ПЗ Plexus й Staffware), Gauss (через інтеграцію з ПО Staffware) і ін.

Пропоновану IDC класифікацію СЕД можна доповнити також системами керування корпоративними електронними записами. Ринковому сегменту ПЗ керування корпоративними записами вже близько 5 років. Корпоративні записи фіксовані в часі й незмінні. Вони є свідченням бізнес-транзакцій, різних прав і зобов'язань й ін. Корпоративні користувачі повинні самі визначити, яке вміст необхідно зробити корпоративним записом (таке рішення вимагає оцінки перспективних потреб їхнього бізнесу). У число корпоративних рішень, що вимагають збереження вмісту, входять основні бізнес-системи, включаючи ERP-системи й бухгалтерські системи, поштові системи (наприклад, MS Exchange), системи керування звітами й висновком, системи електронної комерції, програмні засоби колективної роботи (системи керування проектами, онлайнового конференц-зв'язку й ін.). Як приклади систем керування записами можна привести ПЗ Capture від Tower Software, iRIMS від OpenText й Foremost від TrueArc.

Багатьох важливих функцій керування записами в СЕД раніше не було (наприклад, функцій класифікації). Не були реалізовані також і методи фізичного видалення записів й індексів наприкінці їхнього життєвого циклу (при необхідності). На думку Gartner Group, корпоративним користувачам необхідно доповнити свої Web-сайти функціями систем керування записами. Ряд розроблювачів систем керування Із для підтримки записів Web-сайтів уже розширюють їхня функціональність за допомогою систем керування записами. Роботи в даному напрямку стали особливо помітні в 2002 р. Наприклад, компанія Stellent інтегрувала своє ПЗ керування вмістом із системою керування записами Foremost від компанії TrueArc (слід відзначити, що інтеграція ПЗ керування записами із СЕД досить непроста, тому що необхідно вирішити проблеми дублювання функцій і репозитаріїв). Після такої інтеграції стало можливо робити “знімки” Web-сайту й управляти ними, як записами. Реалізуються й такі цікаві можливості, як запис екранів, що зустрілися під час онлайнової транзакції (наприклад, у ПЗ WebCapture від компанії Tower Technology). Компанія Open Text придбала фірму PS Software (що займається розробкою систем керування записами) і вмонтувала її ПЗ iRIMS як модуль у своє ПЗ LiveLink. Доповнюють своє ПЗ керування вмістом функціональністю систем керування записами також компанії Documentum, IBM й Interwoven (серед інших вендорів ПЗ керування вмістом).

Багато корпоративних користувачів хочуть збирати дані з різних додатків, що працюють у гетерогенному середовищі, і генерувати звіти в електронному виді. Така можливість особливо необхідна для компаній, що використа-

ють ERP-системи (у які завжди збирається й зберігається багато інформації, але не завжди є здатність гнучкої генерації всіх необхідних звітів).

Саме тому на світовому ринку СЕД і з'явилися так називані системи керування висновком (output management systems – OMS), основним призначенням яких є генерація вихідних документів. У деяких OMS-системах додатково реалізовані також можливості архівації й довгострокового зберігання вихідних звітів і документів. У зв'язку із цим, багато хто з OMS-систем класифікуються Gartner Group, як інтегровані системи архівації й пошуку документів (IDARS – integrated document archive and retrieval systems). Однак головною причиною популярності OMS-систем все-таки є займана ними ринкова ніша – генерація документів і звітів в інформаційних системах підприємств й організацій, побудованих з використанням ERP-систем. На думку аналітиків Gartner Group, одним зі слабких місць сучасних ERP-систем є саме погане керування генерацією вихідних документів (розроблювачі ERP-систем більше зосереджені на підвищенні функціональності ключових модулів свого ПЗ, чим на «другорядних» питаннях забезпечення генерації вихідних звітів, що не мають, на їхню думку, гарних ринкових перспектив). Цей недолік ERP-систем і послужив основним фактором появи й швидкого розвитку ринку OMS-систем. Ряд OMS-систем відповідає тільки за розподіл і доставку вихідних документів (в електронному виді - у форматах HTML, XML й PDF). Дуже часто OMS-системи інтегровані із програмними пакетами сканування документів і зображень. Корисною можливістю деяких OMS-систем є й взаємодія з успадкованими корпоративними системами.

Можна також відзначити спеціальні модулі керування електронними документами, що вбудовують в ERP-системи (SAP R/3, Baan й ін.). Однак можливості цих модулів досить обмежені, тому що практично неможливо створити універсальну й повнофункціональну ERP-систему.

Переваги від використання систем електронного документообігу

По даним Forrester Research, 38% компаній зі списку Fortune 500 уважають, що придбання сучасної СЕД є критично важливим для успішного ведення їхнього бізнесу. Відповідно до думки галузевих аналітиків (таких думок, що відрізняються в певних моментах друг від друга, існує досить велика безліч), вигоди для корпоративних користувачів при впровадженні СЕД досить різноманітні. Наприклад, по даним Siemens Business Services, при використанні СЕД:

- Продуктивність праці персоналу збільшується на 20-25%;
- Вартість архівного зберігання електронних документів на 80% нижче в порівнянні з вартістю зберігання паперових архівів.

Прийнято також уважати, що при впровадженні СЕД здобуваються тактичні й стратегічні вигоди. Тактичні вигоди визначаються скороченням витрат при впровадженні СЕД, пов'язаним з: звільненням фізичного місця для зберігання документів; зменшенням витрат на копіювання й доставку документів у паперовому виді; пониженням витрат на персонал й устаткування й ін. До стра-

тегічного ставляться переваги, пов'язані з підвищенням ефективності роботи підприємства або організації. До таких переваг можна віднести:

- поява можливості колективної роботи над документами (що неможливо при паперовому діловодстві);
- значне прискорення пошуку й вибірки документів (по різних атрибутах);
- підвищення безпеки інформації за рахунок того, що робота в СЕД з незареєстрованної робочої станції неможлива, а кожному користувачеві СЕД призначаються свої повноваження доступу до інформації;
- підвищення схоронності документів і зручності їхнього зберігання, тому що вони зберігаються в електронному виді на сервері;
- поліпшення контролю за виконанням документів.

1.3 Уразливість системи електронного документообігу

1.3.1 Об’єкт захисту в електронному документообігу

Електронний документообіг більше уразливий ніж його паперовий попередник: з файлу простіше зробити копію, внести в нього несанкціоновані зміни, виготовити фальшивий документ і т.ін. [6]. Маючи порівняно недороге обладнання, можна організувати атаки на канали зв'язку, на основі яких функціонує СЕД. Крім того, у документообіг організації може бути залучена велика кількість людей, за кожним з яких закріплений ряд виконуваних операцій і група документів, з якого він працює, тобто співробітники виступають у певній ролі щодо системи документообігу. У зловмисника (в основному внутрішнього) виникає багато можливостей для здійснення НСД.

Об'єкт захисту в ЕДО — це файл електронного документа, якому привласнюються звичайні атрибути документа: підпис автора й ступінь його конфіденційності. Цей документ, наприклад, уразливий для модифікації, компрометації або знищення при передачі.

Захист СЕД, які в англійській інтерпретації називаються системами електронного обміну даними (EDI), припускає більше розширений, ніж класичний, підхід до забезпечення ІБ: до понять конфіденційності, цілісності й доступності тут додаються два нових поняття — “законність здійснюваних операцій” й “їх контрольованість”.

Для СЕД виділяють два великих класи атак — атаки на сам зміст електронного документа й на ЕЦП, використовуваний для його запевняння.

1.3.2 Загрози змісту електронного документа

Загрози змісту документа є класичними — це загрози конфіденційності, цілісності й доступності. Вони в цьому випадку дуже різноманітні, наприклад:

- розрив або збій (дисфункція мережі);
- модифікація інформації;
- маскування з метою видати себе за авторизованого відправника або одержувача інформації;

- багаторазове повторення повідомлення;
- розголошення інформації;
- аналіз робочого навантаження лінії зв'язку;
- порушення захисту передачі, при якому погіршуються різні параметри системи безпеки мереж;
- незаконний доступ до аудиторських журналів, що дозволяє сховати сліди можливих несанкціонованих доступів (НСД);
- проникнення в центральну систему через мережу з метою зміни програм, знищення або незаконного внесення деякої інформації.

Перераховані загрози в різному ступені наражають на небезпеку доступність, таємність і цілісність інформації.

1.3.3 Загрози електронному підпису

Атаки на ЕП бувають чотирьох видів.

1. Атаки на криптоалгоритми, пов'язані з можливими помилками, допущеними людьми при їхній розробці.
2. Атаки на криптосистему, під якою звичайно розуміється не тільки використовуваний алгоритм вироблення й перевірки ЕП, але також механізм генерації й розподілу ключів і ряд інших важливих елементів, що впливають на надійність криптосистеми (можливі атаки на механізм генерації ключів — будуть успішні, якщо датчик випадкових чисел, реалізований у криптосистемі для генерації ключів, недостатньо надійний; інші приклади: викрадення або відновлення секретного ключа й т.ін.).
3. Атаки на реалізацію (атаки на ПЗ, що реалізує криптоалгоритм; атаки для одержання секретного ключа, що може просто зберігатися на жорсткому диску; атаки, здійснювані через відсутність контролю цілісності програми генерації або перевірки ЕП, що дозволяє зловмисникові підробити підпис або результати її перевірки, і т.ін.).
4. Атаки на користувачів (типові приклади соціальної інженерії з метою взнати пароль, одержати ключову дискету й т.ін.).

2 ОСОБЛИВОСТІ ПОБУДОВИ ПОЛІТИКИ БЕЗПЕКИ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

2.1 Загальний підхід до побудови політики безпеки системи електронного документообігу

Загальний підхід до побудови політики безпеки системи електронного документообігу можна сформулювати виходячи з вимог стандарту ISO/IEC 17799 [1,9].

Мета: попередити втрати, модифікацію та несанкціоноване використання електронних документів.

Для захисту електронного документообігу варто застосовувати (по необхідності) спеціальні засоби керування безпекою, оскільки ЕДО з партнерами уразливий стосовно несанкціонованого перехоплення й модифікації інформації. Крім того можливо буде потрібно підтвердження передачі або одержання даних. Необхідно також подбати про захист підключених до мережі комп'ютерних систем від загроз, які виходять від електронного підключення.

Засоби керування безпекою операцій по ЕДО повинні бути погоджені з партнерами й постачальниками додаткових мережних послуг. Для забезпечення сумісності із промисловими стандартами, необхідно проконсультуватися з фахівцями відповідною асоціацією по ЕОД.

Для забезпечення конфіденційності даних, що потребують особливого захисту, необхідно розглянути можливість їхнього шифрування. **Шифрування** - це процес перетворення інформації в зашифрований текст для забезпечення її конфіденційності й цілісності під час передачі або при зберіганні. У цьому процесі використовується алгоритм шифрування й інформація про секретний ключ, що відома тільки зареєстрованим користувачам. Рівень захищеності, забезпечуваний процесом шифрування, залежить від якості алгоритму й таємності ключа.

Шифрування може знадобитися для захисту конфіденційної інформації, що уразлива стосовно несанкціонованого доступу, як під час її передачі, так і при зберіганні. Для визначення необхідності шифрування даних і необхідного рівня захищеності необхідно провести оцінку ризику порушення режиму безпеки. Щоб вибрати підходящі програмні продукти з належним рівнем захищеності й розробити надійну систему керування ключами, варто звернутися за порадою до фахівців.

Автентифікація повідомлень - це метод, використовуваний для виявлення несанкціонованих змін, внесених у передані електронні повідомлення, або їхнього ушкодження. Його можна реалізувати на апаратному або програмному рівні за допомогою фізичного пристрою автентифікації повідомлень або програмного алгоритму.

Можливість автентифікації повідомлень варто розглянути для тих додатків, для яких життєво важливим є забезпечення цілісності повідомлень, наприклад, електронні передачі інформації про кошти або інші електронні обміни даними. Для визначення необхідності автентифікації повідомлень і вибору най-

більш підходящого методу її реалізації необхідно провести оцінку ризику порушення режиму безпеки.

Автентифікація повідомлень не призначена для захисту змісту повідомлень від перехоплення. Для цих цілей підходить шифрування даних, яких можна також використати для автентифікації повідомлень.

Електронний підпис - це спеціальний вид автентифікації повідомлень, звичайно заснований на методах шифрування з відкритим ключем, що забезпечує автентифікацію відправника, а також гарантує цілісність умісту повідомлення.

2.2 Вибір моделі для побудови політики безпеки

2.2.1 Модель забезпечення цілісності Кларка-Вільсона

Модель Кларка-Вільсона з'явилася у результаті проведеного авторами аналізу практичних методів забезпечення цілісності документообігу в комерційних компаніях [2]. На відміну від моделей Байба та Белла-ЛаПадули, вона орієнтована на потреби комерційних замовників, і, за думкою авторів, є більш адекватною до їх вимог, ніж комерційна модель цілісності на основі решіток. Основні поняття даної моделі — це коректність транзакцій та розмежування функціональних обов'язків. Модель задає правила функціонування комп'ютерної системи та визначає дві категорії об'єктів даних та два класи операцій над ними.

Усі дані, що містяться у системі, поділяються на контрольовані та неконтрольовані елементи даних (constrained data items CDI і unconstrained data items — UDI відповідно. Останні містять інформацію, цілісність якої в рамках даної моделі не контролюється (цим і визначається вибір технології).

У подальшому модель вводить два класи операцій над елементами даних: **процедури контролю цілісності** (integrity verification procedures — IVP) і **процедури перетворення** (transformation procedures — TP). Перші з них забезпечують перевірку цілісності контрольованих елементів даних (CDI), інші змінюють склад множини усіх CDI (наприклад, перетворюючи елементи UDI в CDI).

Нарешті, модель містить дев'ять правил, що визначають взаємодії елементів даних та процедур у процесі функціонування системи.

Правило C1. Множина усіх процедур контролю цілісності (IVP) повинна містити процедури контролю цілісності будь-якого елемента даних з множини усіх CDI.

Правило C2. Усі процедури перетворення (TP) повинні бути реалізованими коректно у тому сенсі, що не повинні порушувати цілісності CDI, що оброблюється ними. Крім того, с кожною процедурою перетворення повинен бути зв'язаний список елементів CDI, які допустимо оброблювати даною процедурою. Такий зв'язок установлюється адміністратором безпеки.

Правило E1. Система повинна контролювати допустимість застосування TP до елементів CDI відповідно до списків, що вказані у правилі C2.

Правило E2. Система повинна підтримувати список процедур перетворення, дозволених конкретним користувачам, із зазначенням допустимого для кожного TP і даного користувача набору елементів CDI, що підлягають обробці.

Правило C3. Список, визначений правилом C2, повинен від повідати вимозі розмежування функціональних обов'язків.

Правило E3. Система повинна автентифікувати усіх користувачів, що пробують виконати будь-яку процедуру перетворення.

Правило C4. Кожна TP повинна записувати в журнал реєстрації інформацію, достатню для відновлення повної картини кожного застосування цієї TP. Журнал реєстрації — це спеціальний елемент CDI, призначений для додавання до нього інформації.

Правило C5. Будь-яка TP, що обробляє елемент UDI, повинна виконувати тільки коректні перетворення цього елементу, у результаті яких UDI перетворюється в **CDI.**

Правило E4. Тільки спеціальна уповноважена особа може змінити списки, визначені у правила C2 і E2. Ця особа не має права виконувати будь-які дії, якщо вона уповноважена змінювати списки, що регламентують ці дії.

2.2.2 Модель політики безпеки систем електронного документообігу на основі моделі забезпечення цілісності Кларка-Вільсона

Роль кожного з дев'яти правил моделі Кларка-Вільсона (див. 2.2.1) у забезпеченні цілісності інформації можна пояснити, якщо показати, яким з теоретичних принципів політики контролю цілісності відповідає дане правило.

Звичайно для моделі Кларка-Вільсона вибирають перші шість з дев'яти абстрактних теоретичних принципів [2]:

1) коректність транзакцій;
2) автентифікація користувачів;
3) мінімізація привілеїв;
4) розмежування функціональних обов'язків;
5) аудит подій, що відбулися;
6) об'єктивний контроль;
7) управління передачею привілеїв;
8) забезпечення неперервної працездатності;
9) простота використання захисних механізмів.

Для розуміння правил моделі розкриємо дані принципи.

Поняття **коректності транзакцій** звичайно визначається наступним чином. Користувач не повинен модифікувати дані довільно, а тільки визначеними способами, так, щоб зберігалася цілісність даних. Іншими словами, дані можна змінювати тільки шляхом коректних транзакцій і не можна довільними засобами. Крім того. Передбачається, “коректність” (у звичайному сенсі) кожної з таких транзакцій може бути деяким способом доведеною. Принцип коректних транзакцій за своєю суттю відбиває основну ідею визначення цілісності даних,

що ні одному користувачеві системи, у тому числі авторизованому, не повинні бути дозволеними такі зміни даних, які спричинять їх руйнування або втрату.

Другий принцип говорить, що зміни даних може здійснювати користувач, якого спеціально автентифікують для цього. Цей принцип працює разом з наступними чотирма, з якими тісно зв'язана його роль у загальній схемі забезпечення цілісності.

Ідея мінімізації **привілеїв** з'явилася ще на ранніх етапах розвитку напрямку комп'ютерної безпеки у формі обмеження, що накладаються на можливості процесів, що виконуються в системі, і припускають, що процеси повинні бути наділеними тими і тільки тими привілеями для виконання процесів. Практикам адміністрування операційної системи UNIX це положення дуже знайоме на прикладі використання облікового запису, що має необмежені повноваження. Принцип, відповідно до якого слід мінімізувати привілеї, що призначаються, у суворій відповідності із змістом завдання, що виконується, розповсюджується в рівній мірі як на процеси (працюючі в системі програми), так і на користувачів системи.

Розмежування функціональних обов'язків припускає організацію роботи з даними таким чином, що у кожній з ключових стадій, які складають єдиний критично важливий з точки зору цілісності процес, необхідна участь різноманітних користувачів. Цим гарантується, що один користувач не може виконувати весь процес цілком (або навіть дві його стадії) з тим, щоб порушити цілісність даних. У звичайному випадку прикладом втілення даного принципу служить передача однієї половини паролю для доступу до програми керування ядерним реактором першому системному адміністратору, а другий — другому.

Як відзначалося вище, принцип мінімізації привілеїв розповсюджується і на програми, і на користувачів. Останнім, проте, на практиці важко визначити “теоретично досяжний” мінімальний рівень привілеїв за двома причинами. По-перше, користувачі виконують різноманітні завдання, які потребують різних привілеїв. По-друге, якщо суворе дотримання принципу мінімізації у відношенні процесів зв'язане з міркуваннями щодо вартості та продуктивності. То у відношенні користувачів воно. Скоріше, зачіпає питання етики та моралі, а також зручності та ефективності роботи — це фактори, які не піддаються точній кількісній оцінці. Тому користувачі будуть, як правило, мати дещо більше привілеїв, ніж їх необхідно для виконання конкретної дії на даний момент часу. А це відкриває можливості для зловживань.

Аудит подій, що відбулися (включаючи можливість відновлення повної картини подій, що відбулися) є превентивною мірою по відношенню до потенційних порушників.

Принцип **об'єктивного контролю** також є одним з наріжних каменів політики контролю цілісності. Суть даного принципу полягає у тому, що контроль цілісності даних має смисл лише тоді, коли ці дані відображають реальне положення речей. Очевидно, що нема смислу турбуватися про цілісних даних, з розташуванням бойового арсеналу, який уже відправлений на переплавку. У зв'язку з цим Кларк та Вільсон указують на необхідність регулярних перевірок, ме-

тою яких є виявлення можливих невідповідностей між даними, що захищаються, та об'єктивною реальністю, яку вони відображають.

Управління передачею привілеїв необхідне для ефективної роботи усієї політики безпеки. Якщо схема призначення привілеїв неадекватно відображає організаційну структуру підприємства або не дозволяє адміністраторам гнучко маніпулювати нею для забезпечення ефективності виробничої діяльності, захист стає важким тягарем та провокує спроби обійти її там, де вона заважає "нормальній" роботі.

З деякими застереженнями іноді в основу контролю цілісності закладається принцип забезпечення безперервної роботи (включаючи захист від збоїв, стихійних лих та інших форс мажорних обставин), який у класичній теорії комп'ютерної безпеки відноситься, скоріше, до проблеми доступності даних.

В основу дев'ятого принципу **контролю цілісності** — простота використання захисних механізмів — закладений ряд ідей, призваних забезпечити ефективне застосування наявних механізмів забезпечення цілісності. На практиці часто виявляється, що передбачені в системі механізми безпеки некоректно використовуються або повністю ігноруються системними адміністраторами за наступних причин:

- неправильно вибрані виробниками конфігураційні параметри за умочанням забезпечують слабкий захист;
- погано розроблені інтерфейси керування захистом ускладнюють використання навіть простих засобів захисту;
- наявні засоби безпеки не забезпечують адекватний рівень контролю за системою;
- реалізація механізмів безпеки погано відповідає їх інтуїтивному розумінню, що склалося у адміністраторів;
- окремі засоби захисту погано інтегровані в загальну схему безпеки; адміністратори недостатньо поінформовані про важливість застосування конкретних механізмів захисту та їх особливостях.

Простота використання механізмів захисту припускає, що найбільш безпечний шлях експлуатації системи буде також найбільш простим, і навпаки, найбільш простий — найбільш захищеним.

Відповідність правил моделі Кларка-Вільсона до перелічених принципів показані у таблиці 2.1. Як видно із таблиці 2.1 принципи 1 (коректність транзакцій) і 4 (розмежування функціональних обов'язків) реалізуються більшістю правил, що відповідають основній ідеї моделі.

Таблиця 2.1 - Відповідність правил моделі Кларка-Вільсона до принципів політики контролю цілісності

Правило моделі Кларка-Вільсона	Принципи політики контролю цілісності, що реалізуються правилом
Правило С1	Коректність транзакцій Об'єктивний контроль
Правило С2	Коректність транзакцій

Правило E1	Мінімізація привілеїв
	Розмежування функціональних обов'язків
Правило E2	Коректність транзакцій
	Автентифікація користувачів
	Мінімізація привілеїв
	Розмежування функціональних обов'язків
Правило C3	Розмежування функціональних обов'язків
Правило E3	Автентифікація користувачів
Правило C4	Аудит подій, що відбулися
Правило C5	Коректність транзакцій
Правило E4	Розмежування функціональних обов'язків

Публікація опису моделі Кларка-Вільсона викликала широкий відгук серед дослідників, що займаються проблемою контролю цілісності. У ряді робіт розглядаються практичні аспекти застосування моделі, запропоновані деякі її розширення та способи інтеграції з іншими моделями безпеки.

2.3 Засоби правління безпекою систем електронного документообігу

Менеджер безпеки повинен управляти списками контролю доступу до сховища, папкам з файлами, документам, їхнім версіям, системним даним, внесеним на згадку критеріям пошуку, варіантам дизайну, а також до протоколів роботи користувачів, їхніх груп і системи клієнт/сервер [8]. Він також контролює створення, каталогізацію й складання звітів по протоколах безпеки роботи користувальницької й серверної платформ.

2.3.1 Процеси керування списками контролю доступу

Процеси керування списками контролю доступу виконують функції по забезпеченню безпеки роботи додатків СЕД. Безпека всіх об'єктів, якими управляє система, контролюється за допомогою цих функцій. На рисунку 2.1 наведена схема, що ілюструє процеси керування списками контролю доступу.

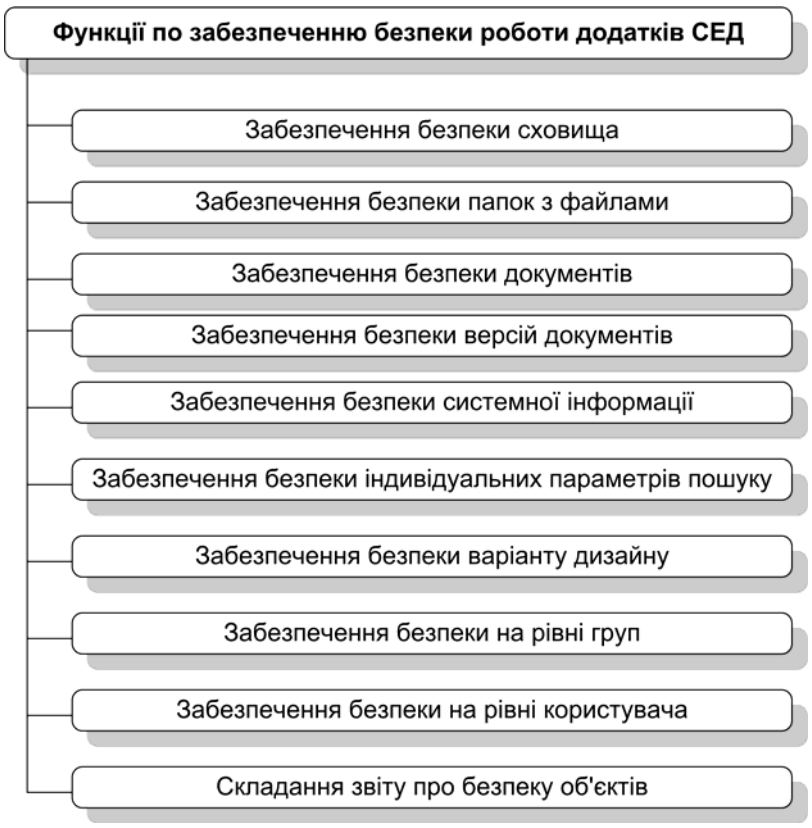

Рисунок 2.1 - Процеси керування списками контролю доступу.

Забезпечення безпеки сховища. Процес забезпечення безпеки сховища запускає системний адміністратор. У ході процесу ведеться загальний контроль доступу окремих користувачів й їхніх груп до сховища.

Забезпечення безпеки папок з файлами. Адміністратор записів запускає процес забезпечення безпеки папок з файлами для здійснення загального контролю доступу до них користувачів і груп. Користувальницький доступ може бути встановлений на рівні *Дозволені читання* або *Доступ заборонений*, у той час як для адміністратора записів можуть установлюватися значення *Дозволене читання*, *Дозволена запис, Дозволені редагування* або *Доступ заборонений*. У питаннях допуску діє принцип наслідування. Наприклад, якщо доступ до папки дозволений тільки певній групі користувачів, то й доступ до всіх документів, розміщеним у цій папці, мають тільки користувачі із зазначеної групи, якщо інше не обговорено на рівні захисту конкретного документа.

Забезпечення безпеки документа. Кінцевий користувач або адміністратор записів запускає процес забезпечення безпеки документа для здійснення загального контролю доступу до нього користувачів і груп. Користувальницький або груповий доступ може бути встановлений на рівні *Дозволене читання, Дозволена запис, Дозволені редагування* або *Доступ заборонений*. У цьому випадку принцип спадкування не має зворотної дії. Наприклад, користувачеві може бути дозволений доступ до документа, але не до папки, що містить цей документ. Таку можливість важливо передбачити на той випадок, якщо користувачеві буде потрібно той або інший документ, і при цьому його не буде цікавити місце розташування цього документа в системі класифікації файлів.

Забезпечення безпеки версії документа. Кінцевий користувач або адміністратор записів запускає процес забезпечення безпеки версії документа для здійснення загального контролю доступу до неї користувачів і груп. Користувальницький або груповий доступ може бути встановлений на рівні *Дозволене читання, Дозволена запис, Дозволені редагування* або *Доступ заборонений*. Певним користувачам може бути наданий доступ до всім розміщеним у комп'ютерній мережі версіям на рівні *Дозволене читання, запис і редагування* (наприклад, фахівці з аналізу політики фірми мають допуск до всіх версій відповідних документів), а інші мають допуск тільки до останніх версій документів на рівні *Дозволене тільки читання*.

Забезпечення безпеки системної інформації. Кінцевий користувач або адміністратор записів запускає процес забезпечення безпеки системної інформації для здійснення загального контролю доступу до неї користувачів і груп. Користувальницький або груповий доступ може бути встановлений на рівні *Дозволене читання, Дозволена запис, Дозволені редагування* або *Доступ заборонений*. Таку можливість важливо передбачити в організаціях, що працюють за принципом "знання по необхідності", відповідно до якого користувачі можуть упевнитися в існуванні певного документа, виходячи із системних відомостей про нього, але для того, щоб побачити сам документ, вони повинні одержати відповідний дозвіл від автора.

Забезпечення безпеки індивідуальних параметрів пошуку. Кінцевий користувач або адміністратор записів запускає процес забезпечення безпеки індивідуальних параметрів пошуку для здійснення загального контролю доступу користувачів і груп до внесеного на згадку системи для повторного використання критеріям пошуку. Користувальницький або груповий доступ може бути встановлений на рівні *Дозволене читання*, *Дозволений запис, Дозволене редагування* або *Доступ заборонений*. Таку можливість варто передбачити в системах, що дозволяють користувачам створювати й запам'ятовувати власні шаблони пошуку, а також передбачають можливість багаторазового використання загальних шаблонів поруч користувачів. Крім того, таким чином, забезпечується контроль за повноваженнями редагувати або видаляти індивідуальні параметри пошуку.

Забезпечення безпеки варіанта дизайну. Кінцевий користувач або адміністратор записів запускає процес забезпечення безпеки варіанта дизайну для здійснення загального контролю доступу користувачів і груп до розташування полів системної інформації. Користувальницький або груповий доступ до версії дизайну може бути встановлений на рівні *Дозволене читання, Дозволена запис, Дозволені редагування* або *Доступ заборонений*. Таку можливість варто передбачити в системах, що дозволяють користувачам створювати й запам'ятовувати власні варіанти дизайну, а також передбачають можливість допуску користувачів до загальних версій подання. Крім того, у такий спосіб забезпечується контроль за повноваженнями редагувати або видаляти варіанти

Забезпечення безпеки на рівні груп. Системний адміністратор запускає процес забезпечення безпеки на рівні груп, щоб ідентифікувати певних членів групи. Члени групи — це користувачі з однаковими обмеженнями на рівень доступу до функцій пошуку документів, системних даних, варіантів дизайну й так

далі. Всім членам групи привласнюється найвищий рівень допуску, установлений для групи. Наприклад, якщо користувач Петренко має доступ до документа на рівні *Дозволено тільки читання*, і при цьому він входить до складу групи, який *Дозволене читання й запис*, то Петренку також буде привласнене право *Запису*, як члену відповідної групи.

Забезпечення безпеки на рівні користувача. Системний адміністратор запускає процес забезпечення безпеки на рівні користувача, щоб установити атрибути рівня доступу для конкретного користувача або адміністратора. У цьому випадку доступ користувача до документів, системним даним, варіантам дизайну й так далі контролюється в індивідуальному порядку. Змінна контролю доступу може, як правило, приймати наступні значення: *Доступ заборонений, Дозволене читання, читання/запис, запис, редагування й видалення*.

Складання звіту про безпеку об'єктів. Системний адміністратор запускає процес складання звіту про безпеку об'єктів, щоб підсумувати й скласти загальний огляд списків контролю доступу й станів об'єктів СЕД. У число об'єктів входять сховища, папки з файлами, документи, їхні версії, системна інформація, шаблони пошуку, варіанти дизайну й безпека на рівні груп й окремих користувачів. Як правило, для виконання цієї функції в системі передбачений убудований генератор звітів. У противному випадку можна здійснити запит бази даних, де зберігається інформація, за допомогою окремої програми.

2.3.2 Процеси забезпечення безпеки протоколів роботи

Процеси забезпечення безпеки протоколів роботи (див. рисунок 2.2) відповідають за протоколювання подій, що відбуваються в користувальницькому або серверному середовищі. Ця функція може бути успадкована від компонентів середовища СЕД. У противному випадку, “поверх” відповідних додатків може бути встановлена окрема програма, наприклад, монітор контролю взаємодії, що буде протоколювати всі здійснювані в рамках системи дії й відправляти їх у базу даних, де їх зможуть переглянути співробітники групи безпеки.

Забезпечення безпеки протоколу роботи користувача. Системний адміністратор запускає процес забезпечення безпеки протоколу роботи користувача, щоб обмежити доступ до протоколу дій, що виконувалися в користувальницькому середовищі. Протоколи роботи користувача повинні записуватися у форматі, відмінному від ASCII, і необхідно виключити можливість перегляду протоколів для кінцевих користувачів, щоб звести до мінімуму кількість людей, обізнаних про дії й події, інформацію про які можна несумлінно використати.

Складання звіту про безпеку протоколу роботи користувача. Системний адміністратор запускає процес складання звіту про безпеку протоколу роботи користувача, щоб підсумувати й скласти загальний огляд протоколів дій, що здійснювалися в користувальницькому середовищі. Для перегляду інформації повинне бути досить монітора контролю взаємодії або убудованого генератора звітів. Проте, іноді виникають ситуації, коли групі забезпечення безпеки може знадобитися переглянути повний список операцій, що виконувалися, щоб у то-

чності відтворити послідовність екранів програми або дій, що виконувалися на комп'ютері кінцевого користувача.

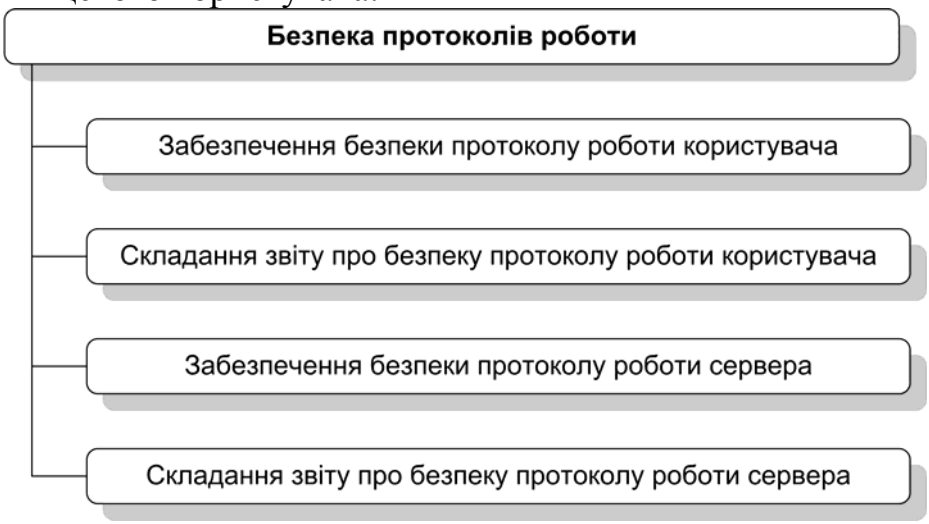

Рисунок 2.2 - Процеси забезпечення безпеки протоколів роботи.

Забезпечення безпеки протоколу роботи сервера. Системний адміністратор запускає процес забезпечення безпеки протоколу роботи сервера, щоб обмежити доступ до протоколу дій, що виконувалися в серверному середовищі. Така можливість повинна бути надана тільки дуже обмеженій групі адміністраторів систем безпеки.

Складання звіту про безпеку протоколу роботи сервера. Системний адміністратор запускає процес складання звіту про безпеку протоколу роботи сервера, щоб підсумувати й скласти загальний огляд протоколів дій, що здійснювалися в серверному середовищі. Як й у випадку з користувальницькими протоколами, для перегляду інформації повинне бути досить монітора контролю взаємодії або убудованого генератора звітів.

2.4 Основні правила безпеки системи електронного документообігу

СЕД повинна бути захищена від зловживань і від проникнення в систему неавторизованих користувачів, і при цьому міри безпеки не повинні перешкоджати виконанню користувачами своїх обов'язків. У деяких системах процедура підключення клієнта до мережі дуже поверхнева, і кінцевий користувач може легко змінити параметри цієї процедури. З погляду забезпечення безпеки такі системи не представляються досить потужними. У деяких випадках на серверах спостерігається прямо протилежна ситуація - міри безпеки настільки строгі, що в результаті утворюються затори в роботі. Раціонально організована процедура входу в систему й складання звітності (або, принаймні, використання програмних “гачків” за допомогою інтерфейсу API) дозволить підприємству запустити різні стандартні програми, що задовольняють потребам даної конкретної фірми.

У СЕД повинна бути передбачена можливість простежування історії будь-якого документа. Кожен компонент сховища СЕД, у якому розміщаються інші об'єкти, повинен мати протокол, у якому вказується, хто одержував доступ до об'єктів і редагував їх. Така система забезпечує можливість проконтролювати

кожен об'єкт і визначити співробітника, що останнім переглядав і редагував документ.

Контроль доступу - це першочергове завдання систем керування документацією. За нею треба ще один важливий момент - організація системи перевірки повноважень осіб, що володіють певними правами. Необхідно контролювати доступ до всіх баз - базі документів, базі даних і текстовій базі. Всі вони повинні підкорятися єдиному механізму контролю доступу; у противному випадку співробітник, що має доступ тільки до комп'ютерної мережі, міг би обійти системи захисту додатків і без обмежень скористатися пошуковим механізмом бази даних. Таким чином, з'явилася б можливість визначити, чи існує документ, і, скориставшись його ідентифікатором, одержати його з якої-небудь іншої області комп'ютерної мережі.

Можливості контролю доступу зростають, якщо самі документи зберігаються в системі окремо від бази даних їхніх системних описів. Такий варіант поділу системних функцій представляється дуже зручним, оскільки в деяких випадках організація надає користувачеві право запитувати базу даних за системною інформацією, але не відкриває доступу до самих документів. Якщо документи й системні описи зберігаються в одній базі даних, зростає ймовірність порушення встановлених правил. Якщо людина вийшла на базу даних, те, найімовірніше, він зуміє добратися й до документів.

Система контролю доступу на рівні вмістищ (ієрархічних щаблів, що відповідають приміщенню, шафі, ящику, папці й документу) установлює обмеження на список осіб, що мають право переглядати документ, вносити в нього зміни або видаляти його. Контроль доступу певних співробітників або їхніх груп повинен бути обмежений за допомогою визначення прав групи на перегляд і створення документів. Необхідно знайти спосіб звіряти паролі при вході користувача в систему. У загальному випадку існує два способи здійснити таку перевірку: перший - задати окремий пароль для додатка, другий - дозволити доступ до додатка всім користувачам, які вже підключилися до мережі, не змушуючи їх одержувати для цього авторизацію другий раз.

Можна також установити систему контролю доступу до окремих функцій програмного забезпечення (таким як перегляд, роздруківка, копіювання, установка й зняття обмежень на доступ, видалення й так далі). Різним користувачам можна надати різний рівень доступу.

Система моніторингу відповідає не тільки за контроль доступу; вона також може стежити за повсякденними операціями в рамках СЕД, щоб запобігти несанкціонованим діям. Система може контролювати важливі зміни, які вносяться в процесі експлуатації СЕД користувачем або адміністратором, і вчасно попередити групу забезпечення безпеки, якщо нормальний плин тієї або іншої процедури було порушено. Наприклад, якщо документи в системі видаляються після певної кількості переглядів, співробітник може забрати зі сховища й повернути назад документ 40 разів, щоб одержати можливість знищити оригінал документа, у якому втримується інформація про неправомірні дії цієї людини - і в результаті первісний документ разом зі свідченнями, що втримувалися в ньому, винності зникне.

Останній елемент, що обов'язково повинен бути присутнім у системі безпеки - функція перевірки вірогідності електронного підпису співробітника на документі й незмінності цього підпису з моменту створення оригіналу документа. Як правило, це робиться за допомогою установки взаємозв'язку електронного підпису з оригіналом документа з використанням певних математичних методів. Якщо відбувається розрив зв'язку, автоматично встановлюється попереджуючий знак, що говорить про те, що документ підроблений.

2.1.5 Типовий комплекс засобів захисту системи електронного документообігу

Для захисту СЕД використаються традиційні засоби:

- ідентифікація, автентифікація й авторизація об'єктів і суб'єктів (так, до питань авторизації в СЕД ставляться механізми розмежування доступу до даних і функцій системи — це, наприклад, наявність можливості в керівника відділу переглядати всі документи, над якими працюють співробітники відділу, у той час як кожен співробітник бачить лише свою частину роботи й не бачить документи, над якими працюють інші; кожний з документів може мати встановлені для нього права доступу на читання, зміну, видалення; корисно виділяти групи користувачів і делегувати права їхнього доступу до документів);
- керування доступом (дозволяє визначати для кожного документа й для кожної ПП правочинних користувачів й їхнього права);
- мережне екранування;
- засоби контролю імпортованих програм;
- криптографія;
- електронний цифровий підпис.

Розглянемо ці засоби стосовно до захисту від різних загроз.

Захист ЕДО від загроз конфіденційності здійснюється за допомогою стеганографії й криптографії. Стеганографія займається проблемою приховання від зловмисника самого факту передачі повідомлення. Найчастіше це досягається за рахунок введення в повідомлення додаткових бітів, що не псує якості зображення. Виявити заховане в такий спосіб повідомлення малого обсягу у великому обсязі інформації, не знаючи методу приховання й не маючи “чистого” варіанта файлу, досить складно. Загальний недолік стеганографічних методів захисту інформації — проблема збереження в таємниці самого методу приховання.

Криптографія має на меті приховання тексту повідомлення, роблячи його не читають для небажаних очей. При цьому допускається, що зловмисник знає не тільки сам факт передачі повідомлення, але й саме повідомлення, можливо, його приблизний або навіть точний текст. Допускається знання супротивником методу шифрування. У таємниці від зловмисника повинен залишатися тільки секретний параметр шифрування — ключ.

Для СЕД найчастіше застосовується два підходи.

1. Абонентське шифрування конфіденційної інформації — шифрування переданих між абонентами ІТС електронних документів. Використається схема

абонентського шифрування із закритим розподілом ключів шифрування між абонентами, на базі повної матриці ключів (кожній парі абонентів системи відповідає свій секретний ключ для передачі шифрованих документів між ними). Достоїнство цього методу в тім, що алгоритм шифрування забезпечує доступ до переданої інформації тільки тим особам, яким дана інформація призначена.

2. Комплексний захист конфіденційності переданих між абонентами ІТС електронних документів з одночасним стиском (архівуванням) документів, забезпеченням їхньої цілісності й автентифікація автора за допомогою ЕЦП. Обробка документів виробляється безпосередньо перед передачею або після прийому їхніми звичайними засобами електронної пошти.

Захист цілісності ЕДО ділиться на підзавдання захисту від несанкціонованої зміни, підробки й пропажі. Рішення перших двох проблем здійснюється застосуванням ЕЦП, заснованої на криптографії з відкритим ключем. Рішення проблеми пропажі документа лежить поза криптографією — тут потрібне створення резервних копій з носіїв інформації, їхнє дублювання й строгий облік документів. При передачі документа по каналах зв'язку потрібні захищені протоколи передачі даних (типу SSL, TLS або інших), що надають можливості одержання підтвердження про доставку, що здійснюють передачу даних різними маршрутами, і т.ін.

Захист ЕДО від загроз доступності, або від атак типу “відмова в обслуговуванні”, реалізується на рівні операційної системи, програмного й апаратного забезпечення установкою відповідних “латок”. Загроза полягає у відмові легальному (санкціонованому) користувачеві одержати доступ до інформації з боку системи. Способів створити ситуацію відмови в обслуговуванні, як буде описано далі, багато, починаючи від примітивних багаторазових спроб входу в систему від імені користувача до блокування його облікового запису й закінчуючи застосуванням хакерських атак на сервер типу “затоплення” повторюваними пакетами.

Підкреслимо, що захист СЕД досягається не окремими рішеннями, а системою добре продуманих мер, включаючи комплекс адміністративних процедур. Можливі створення системи захисту СЕД як єдиного цілого або розробка підсистем безпеки для окремих інформаційних комплексів СЕД. Незалежно від цього СЕД повинні мати рішення по забезпеченню ІБ у таких важливих областях застосування, як, наприклад, планування відновлення після НСД, розподілене зберігання даних, керування пристроями й сховищами даних, резервне копіювання й архівування й багато чого іншого.

2.2 Обґрунтування комплексу засобів захисту системи управління базами даних електронного документообігу

2.2.1 Основні вимоги до комплексу засобів захисту системи управління базами даних

Виходячи із загальних вимог до побудови політики та враховуючи [] можна сформулювати загальні вимоги до комплексу засобів захисту системи управління базами даних електронного документообігу.

Основні вимоги повинні забезпечувати базову функціональність бази даних, включаючи надання можливості одним користувачам одержати дискреційне право надавати інформацію, до якої вони мають законний доступ, іншим користувачам.

Адміністратори цих систем повинні мати можливість:

- управляти й постійно контролювати дії кінцевих користувачів, щоб сприяти запобіганню порушення їхніх прав у межах системи;
- управляти споживанням ресурсу індивідуальними користувачами, і
- ураховувати дії користувачів.

Автентифікаційні пакети мають надавати засоби для підтвердження дійсності користувача:

- Автентифікація в операційній системі (користувач автентифікований ОС хоста й ідентифікований у базі даних); або
- Автентифікація в базі даних (користувач ідентифікований й автентифікований СУБД).

Підхід поділу основних вимог й автентифікаційних пакетів прийнятий для того, щоб спростити супровід вимог захисту. Це припускає, що в майбутніх вимогах захисту список пропонованих автентифікаційних пакетів може розширюватися, наприклад, щоб включити каталог, заснований на автентифікації.

Для того щоб заявити відповідність вимогам захисту в завданні з безпеки, повинно бути встановлено, який необхідно затвердити автентифікаційний пакет. Заяка відповідності ПЗ повинні встановлювати або “СУБД у режимі автентифікації засобами ОС”, або “СУБД у режимі автентифікації засобами бази даних”, або “СУБД у режимі автентифііікації засобами ОС і засобами бази даних”.

2.2.2 Опис системи управління базами даних як об’єкта оцінки інформаційної безпеки

Головні особливості

Звичайно СУБД використовується для того, щоб надати багатьом користувачам одночасний доступ до бази даних [7].

СУБД може бути сконфігурована багатьма способами:

- автономна система з одиночним користувачем бази даних (наприклад, додаток, заснований на роботі окремого користувача на персональному комп'ютері);
- багато користувачів бази даних, що працюють за терміналами, які пов'язані із центральною машиною (наприклад, традиційний варіант термінал - середовище мейнфрейма);
- мережа інтелектуальних робочих станцій, що підтримують зв'язок із центральним сервером (архітектура “клієнт-сервер”); або
- мережа інтелектуальних клієнтських робочих станцій, що підтримують зв'язок з додатком сервера, що у свою чергу пов'язане із СУБД (наприклад, Web-браузер, що підтримує зв'язок з Web-сервером, що формує динамічні сторінки за допомогою СУБД).

У кожній з вищезгаданих конфігурацій самі дані можуть постійно перебувати на одному сервері або можуть бути розподілені серед багатьох незалежних серверів.

СУБД являє собою додаток, що використає функції базової системи нижчого рівня (операційної системи хоста й/або мережних сервісів, і/або спеціально замовленого програмного забезпечення), і є IT-компонентом конкретної системи.

Додаток СУБД може складатися з одного або декількох виконуваних завантажувальних модулів й одного або декількох файлів даних. Вони будуть підлеглі адмініструванню основних системних прав, як і будь-які інші основні системні процеси й файли.

СУБД може розширювати функціональні можливості засобів забезпечення безпеки базової системи. Наприклад, база даних може реалізувати набагато кращий розгалужений механізм привілеїв, чим операційна система хоста.

Автентифікаційні пакети

Автентифікаційний пакет надає для бази даних механізм підтвердження дійсності ідентифікатора користувача, що заявляє. У межах даного профілю захисту це може бути забезпечено наступними двома механізмами:

- Зовнішнім – за допомогою операційної системи хоста (автентифікація засобами ОС). У цій схемі автентифікації при ідентифікації й автентифікації користувача база даних покладається на операційну систему хоста, що у цьому випадку забезпечує підтвердження дійсності користувача в базі даних. База даних використає наданий операційною системою ідентифікатор для встановлення ідентифікатора бази даних (які можуть бути різними).
- Безпосередньо в межах бази даних автентифікація засобами бази даних). У цій схемі автентифікації база даних верифікує заявляє ідентифікатор, що, користувача, використовуючи свій власний механізм автентифікації.

Принаймні, один з вищезгаданих сервисов аутентификации повинен бути наданий відповідною базою даних. Середовище безпеки

2.2.3 Опис середовища забезпечення безпеки

Тепер необхідно визначити активи IT, що захищають об’єкт оцінки (ОО). Також визначаються загрози цим активам IT, політика безпеки організації, що підтримує ОО, і припущення безпечного використання ОО.

Активи IT

Активи IT, що вимагають захисту, складаються з інформації, збереженої в межах СУБД, конфіденційність, цілісність або доступність якої може бути скомпрометована.

Активами IT є:

- Об'єкти бази даних і дані, що втримуються в межах цих об'єктів бази даних. Об'єктами БД можуть бути об'єднання частин даних, що втримуються в інших об'єктах бази даних.
- Дані управління базою даних використаються СУБД для того, щоб організувати й захистити об'єкти бази даних.
- Дані аудита бази даних генеруються СУБД у процесі її функціонування.

Загрози

Прийняті загрози безпеки ОО, поряд з порушниками, які могли б провокувати ці загрози, визначені нижче. Усякий виклад загрози ідентифікує засобу, за допомогою яких ОО і його базова система можуть бути скомпрометовані.

Цим загрозам будуть протистояти:

а) технічні заходи безпеки, надані ОО, разом з

б) технічними заходами безпеки, наданими базовою системою й

в) не технічні операційні заходи безпеки в середовищі (процедурні, фізичні міри й стосовні до персоналу).

Порушники

Порушниками можуть бути:

Особи, які не є вповноваженими користувачами базової системи (операційної системи й/або мережних сервісів, і/або спеціального програмного забезпечення).

Особи, які є вповноваженими користувачами ОО.

Особи, які є вповноваженими користувачами базової системи. Користувачами цієї системи можуть бути:

а) особи, які не є користувачами бази даних; або

б) особи, які є користувачами бази даних.

Переривання операцій, що є результатом збоїв апаратних засобів, джерел живлення, носіїв даних і т.д.

Загрози, що запобігаються ОО

Порушники можуть ініціювати наступні типи загроз СУБД (або СУБД повинна протистояти наступним загрозам).

T.ACCESS. Несанкціонований доступ до бази даних. Сторонній або користувач системи, що у цей час не є вповноваженим користувачем бази даних, звертається до СУБД. Ця загроза включає виконання ролі особи, що може або не може бути вповноваженим користувачем бази даних, а також яке звертається до СУБД, виконуючи роль уповноваженого користувача бази даних (включаючи вповноваженого користувача, що виконує роль іншого користувача, що має інший, можливо більше привілейований, доступ).

T.DATA. Несанкціонований доступ до інформації. Уповноважений користувач бази даних звертається до інформації, що втримується в межах СУБД, без дозволу користувача бази даних, що є власником даних або який відповідає за захист даних.

Ця загроза включає несанкціонований доступ до інформації СУБД, залишкової інформації, що зберігається в пам'яті або в ресурсах зберігання, керованих ОО, або до даних управління БД.

T.RESOURCE. Надмірне використання ресурсів. Автентифікований користувач бази даних використає глобальні ресурси бази даних шляхом, що ставить під загрозу можливість інших користувачів бази даних одержати доступ до СУБД.

Ця загроза ставиться до доступності інформації в межах СУБД. Наприклад, користувач бази даних міг виконувати дії, пов'язані з використанням надмірних ресурсів, періодично перешкоджаючи законному доступу інших користувачів бази даних до даних, ресурсам і сервісам. Такі напади можуть бути зловмисними, відбуватися в результаті неуважності або недбалості, або у випадку, коли користувач бази даних може просто не усвідомлювати потенційні наслідки своїх дій. Вплив таких нападів на готовність і надійність системи може бути посилено багатьма користувачами, що діють одночасно.

T. ATTACK. Невиявлений напад. Невиявлена компрометація СУБД відбувається в результаті дій порушника (уповноваженого або з користувача бази даних), що намагається виконати дії, які він не вповноважений виконувати.

Ця загроза включена, тому що незалежно від забезпечення контрзаходів, адресованим іншим загрозам, все-таки є ще залишкова загроза порушення політики безпеки порушниками, що намагаються протистояти цим контрзаходам.

T.ABUSE.USER. Неправильне використання привілеїв. Невиявлена компрометація СУБД відбувається в результаті дій користувача бази даних (навмисних чи ні), пов'язаних з виконанням операцій індивідуума, уповноваженого на їхнє виконання.

Ця загроза включена, тому що незалежно від забезпечених контрзаходів, адресованих іншим загрозам, все-таки є ще залишкова загроза порушення політики безпеки або бази даних, розміщеної в небезпечному місці, у результаті дій, початих уповноваженими користувачами бази даних. Наприклад, користувач бази даних може надати доступ до об'єкта БД, відповідальним за який він є, іншому користувачеві бази даних, здатному використати цю інформацію для шахрайських цілей.

Відзначимо, що ця загроза не поширюється на користувачів бази даних з високим рівнем довіри: див. припущення A.MANAGE нижче.

Загрози, що запобігають середовищем

T.OPERATE. Небезпечна операція. Компрометація бази даних може відбутися через неправильну конфігурацію, адміністрування й/або функціонування складної системи.

T.CRASH. Раптові переривання. Раптові переривання функціонування ОО можуть привести до втрати або руйнування даних, пов'язаних з безпекою, таких як дані управління БД і дані аудита. Такі переривання можуть бути результатом помилки оператора (див. також T.OPERATE) або збоїв програмного забезпечення, апаратних засобів, джерел живлення або носіїв даних.

T.PHYSICAL. Фізичний напад. Критичні до безпеки частини ОО або базової операційної системи й/або мережних сервісів можуть бути піддані фізичному нападу, що може порушити безпека.

Політики безпеки організації

P.ACCESS. Доступ до об'єктів БД визначається:

а) власником об'єкта БД; і

б) ідентифікатором суб'єкта бази даних, що намагається одержати доступ; і

в) привілеями доступу до об'єкта БД, якими володіє суб'єкт бази даних; і

г) адміністративними привілеями суб'єкта бази даних; і

д) ресурсами, виділеними суб'єктові.

Помітимо, що ця політика включає наступне:

а) володіння - власники об'єктів БД відповідальні за свої об'єкти; і

б) дискреційне управління доступом – власники об'єктів БД можуть надавати іншим користувачам бази даних доступ або управління своїми об'єктами БД на основі дискреційного управління доступом; і

с) ресурси - користувачі бази даних уповноважені використати тільки ті ресурси, які розподілені їм.

P.ACCOUNT. Користувачі бази даних відповідальні за:

а) операції на об'єктах, які визначені власником об'єкта; і

б) дії, певні адміністраторами бази даних.

Припущення

ОО залежить як від технічних аспектів ІТ, так і від функціональних аспектів її середовища.

Припущення по ОО

A.TOE.CONFIG. ОО інстальований, сконфигурований й управляється у відповідності зі своєю оціненою конфігурацією.

Основні системні припущення

Фізичні припущення.

A.PHYSICAL. Ресурси функціонування ОО й базової системи розташовані в межах управління засобами доступу, які запобігають несанкціонований фізичний доступ сторонніх, користувачів системи й користувачів бази даних.

Припущення конфігурації.

A.SYS.CONFIG. Базова система (операційна система й/або сервіси безпеки мережі, і/або спеціальне програмне забезпечення) інстальовані, сконфигуровані й управляються у відповідності зі своєю безпечною конфігурацією.

A.ACCESS. Базова система конфігурована так, що тільки санкціонована група осіб може одержати доступ до системи.

A.MANAGE. Будуть призначені одне або більше компетентних довірених осіб для того, щоб управляти ОО, базовою системою й безпекою інформації.

Припущення зв’язності.

A.PEER. Передбачається, що будь-які інші компоненти ИТ, з якими взаємодіє ОО, будуть під тим же самим управлінням і функціонують під тією же самою політикою безпеки.

A.NETWORK. Передбачається, що коли потрібно для ОО, у розподіленому середовищі базові сервіси мережі будуть засновані на безпечних протоколах взаємодії, які забезпечать автентичність користувачів.

2.2.4 Цілі безпеки

Цей розділ описує безпеки ІТ ОО, а також загрози й політики, яким вони адресовані. У ньому далі представлені вимоги до середовища функціонування, необхідні для підтримки цілей ИТ ОО.

Цілі безпеки ІТ

Цей підрозділ визначає цілі безпеки ІТ, які повинні бути задоволені за допомогою ОО в комбінації із середовищем безпеки ИТ. У таблиці 2.2 представлене відношення цілей безпеки ОО до кожної з загроз і політик безпеки й показано, що всякій загрозі відповідає, принаймні, одна мета безпеки ИТ, і що всяка політика безпеки задоволена, принаймні, однією метою безпеки ИТ. У таблиці слово «ТАК» указує, що зазначена мета безпеки ИТ доречна для певної загрози або політики безпеки.

Таблиця 2.2 - Взаємозв'язок загроз і політик із цілями безпеки ОО

Загрози\Політики	O.I&A.TOE	O.ACCESS	O.AUDIT	O.RESOURCE	O.ADMIN .TOE
T.ACCESS	ТАК	ТАК		ТАК	ТАК
T.DATA	ТАК	ТАК			ТАК
T.RESOURCE	ТАК	ТАК		ТАК	ТАК
T.ATTACK	ТАК	ТАК	ТАК		ТАК
T.ABUSE.USER	ТАК	ТАК	ТАК		ТАК
P.ACCESS		ТАК		ТАК	
P.ACCOUNT		ТАК	ТАК		

O.ACCESS. ОО повинен забезпечити кінцевих користувачів й адміністраторів можливістю управління доступом до їхніх власних даних або ресурсів або до тих, за які вони відповідають відповідно до політики безпеки P.ACCESS. Для цього ОО має наступні більше конкретні цілі:

O.ACCESS.OBJECTS. ОО повинен запобігти несанкціонованому або непередбачуваному розкриттю, уведення, модифікацію або знищення даних й об'єктів бази даних, а також перегляд бази даних, управління даними й аудит дані бази даних.

O.ACCESS.CONTROL. ОО повинен надати можливість користувачам бази даних, які є власниками або відповідальними за дані, управляти доступом до цим даних інших уповноважених користувачів бази даних.

O.ACCESS.RESIDUAL. ОО повинен запобігти несанкціонованому доступу до залишкових даних, що залишається в об'єктах і ресурсах після використання цих об'єктів і ресурсів.

O.RESOURCE. ОО повинен надати засоби управління використанням ресурсів бази даних уповноваженими користувачами ОО.

O.I&A.TOE. ОО з підтримкою або без підтримки базової системи повинен надати засоби ідентифікації й автетифікації користувачів ОО.

O.AUDIT. ОО повинен надати засоби докладної реєстрації значимих для безпеки подій для того, щоб у достатній мері допомогти адміністраторові ОО:

а) виявляти початі порушення безпеки або потенційну помилку в конфігурації засобів безпеки ОО, які залишили б базу даних незахищеної від компрометації; і

б) зобов'язати індивідуальних користувачів бази даних бути відповідальними за будь-які виконувані ними дії, які є значимими для безпеки бази даних відповідно до політики P.ACCOUNT.

O.ADMIN.TOE. Там, де необхідно, ОО разом з базовою системою повинен надати функції, що дозволяють уповноваженому адміністраторові ефективно управляти ОО і його функціями безпеки, забезпечуючи, щоб тільки вповноважені адміністратори могли одержувати доступ до такої функціональності.

Цілі безпеки для середовища

Наступні цілі безпеки IT повинні бути задоволені середовищем, у якій ОО використається.

O.ADMIN.ENV. Там де необхідно, ОО разом з базовою системою повинен надати функціональні можливості, що дозволяють уповноваженому адміністраторові ефективно управляти ОО і його функціями безпеки, забезпечуючи, щоб тільки вповноважені адміністратори могли одержувати доступ до такої функціональності.

O.FILES. Базова система повинна забезпечити механізми управління доступом, які дозволять захистити від несанкціонованого доступу всі пов'язані із СУБД файли й каталоги (включаючи виконувані програми, бібліотеки робочих програм, файли бази даних, експортовані файли, файли повторної реєстрації, керовані файли, файли із трасуванням і файли з дампом).

O.I&A.ENV. Базова операційна система повинна надати засоби ідентифікації й автентифікації користувачів, коли потрібно за допомогою ОО надійно підтвердити дійсність користувачів.

O.SEP. Базова операційна система повинна надати засоби для ізоляції функцій безпеки ОО й упевненість у тім, що компоненти ФБО не будуть спотворюватися. Складовими, реалізуючі ФБО, є: 1) файли, використовувані СУБД для того, щоб зберігати базу даних й 2) процеси ОО, що управляють базою даних.

Наступні, не пов'язані з ІТ, мети безпеки повинні бути задоволені процедурними й іншими мірами, початими в межах середовища ОО.

O.INSTALL. Відповідальні за ОО повинні забезпечити, щоб:

а) ОО був поставлений, інстальований, управлявся й використався відповідно до експлуатаційної документації ОО, і

б) Базова система була інстальована й використалася відповідно до її експлуатаційної документації. Якщо елементи системи сертифіковані, то вони повинні бути інстальовані й використатися відповідно до необхідної документації сертифікації.

O.PHYSICAL. Відповідальний за ОО повинен забезпечити, щоб ті частини ОО, які є критичними до політики безпеки, були захищені від фізичного нападу.

O.AUDITLOG. Адміністратори бази даних повинні забезпечити, щоб засобу аудита використалися й управлялися ефективно. Ці процедури повинні застосовуватися в журналі аудита бази даних й/або журналі аудита для базової операційної системи, і/або для мережних сервісів безпеки. Особливо:

а) повинні бути початі необхідні дії для того, щоб забезпечити тривале функціонування аудита, наприклад, для того, щоб забезпечити достатню вільну пам'ять, необхідну для регулярної архівації журналу аудита;

б) журнали реєстрації подій аудита повинні регулярно проглядатися й необхідно визначити дії або події, які можуть привести до порушення безпеки в майбутньому.

в) системний годинник повинні бути захищені від несанкціонованої модифікації (так, щоб цілісність міток часу аудита не була скомпрометована).

O.RECOVERY. Відповідальний за ОО повинен надати можливість для процедур й/або механізмів відновлення функціонування на місці після системного збою або іншого переривання без компромісу із захистом.

O.QUOTA. Адміністратори бази даних повинні забезпечувати, щоб кожен користувач ОО мав необхідні квоти, які:

а) достатні для виконання операцій, до яких користувач має доступ;

б) досить обмежені, щоб користувач не міг порушити режим експлуатації, доступ до ресурсів і монополізувати ресурси.

O.TRUST. Відповідальний за ОО повинен забезпечити, щоб тільки в користувачів з високим рівнем довіри був привілей, що дозволяє їм:

а) установлювати або змінювати конфігурацію журналу аудита для бази даних;

б) змінювати або видаляти будь-який запис аудита в журналі аудита бази даних;

в) створювати будь-які облікові дані користувача або змінювати будь-які атрибути безпеки користувача;

г) надавати на повноваження використання адміністративних привілеїв.

O.AUTHDATA. Відповідальний за ОО повинен забезпечити, щоб дані автентифікації для будь-яких облікових даних користувача ОО, так само як і для базової системи, надійно підтримувалася й не розкривалися особам, які не вповноважені використати цей обліковий запис. Особливо:

Таблиця 2.3 - Відображення цілей безпеки середовища на загрози, мети безпеки ОО, політику й припущення про безпечне використання

Цілі безпеки середовища	Протистояча загроза	Підтримувана ціль ОО	Підтримувана політика	Відображення в припущенні про безпечне використання
O.INSTALL	T.OPERATE			A.TOE.CONFIG, A.SYS.CONFIG, A.MANAGE
O.PHYSICAL	T.PHYSICAL			A.ACCESS, A.PEER, A.PHYSICAL
O.AUDITLOG		O.AUDIT	P.ACCOUNT	A.MANAGE
O.RECOVERY	T.CRASH			A.MANAGE
O.QUOTA		O.RESOURCE		A.MANAGE
O.TRUST			P.ACCESS	A.MANAGE
O.AUTHDATA		O.I&A.TOE	P.ACCESS	A.MANAGE, A.PEER, A.NETWORK
O.MEDIA	T.CRASH			A.MANAGE
O.ADMIN.ENV		O.ADMIN.TOE		A.MANAGE
O.FILES	T.ACCESS		P.ACCESS	A.MANAGE
O.I&A.ENV	T.ACCESS	O.I&A.TOE	P.ACCESS	A.MANAGE
O.SEP	T.ACCESS		P.ACCESS	A.MANAGE

а) носії, на яких зберігаються дані автентифікації для базової операційної системи й/або мережних сервісів безпеки, не повинні бути фізично переборні з базової платформи несанкціонованими користувачами;

б) користувачі не повинні розкривати свої паролі іншим особам;

в) паролі, згенеровані адміністратором системи, повинні бути розподілені безпечним способом.

O.MEDIA. Відповідальний за ОО повинен забезпечити, щоб конфіденційність, цілісність і доступність даних, збережених на носіях даних, були адекватно захищені. Особливо:

а) мережні й автономні пристрої зберігання даних, на яких розташовується база даних і дані, пов'язані з безпекою (такі як, резервні копії операційної системи, резервні копії бази даних, журнали транзакцій і журнали аудита), фізично не могли бути несанкціоновано усунуті з базової платформи користувачами.

б) мережні й автономні пристрої зберігання даних повинні підходящим образом зберігатися й підтримуватися, а також регулярно перевірятися для того, щоб забезпечити цілісність і доступність пов'язаних з безпекою даних.

в) носії, на яких зберігаються пов'язані з базою дані файли (включаючи файли бази даних, експортні файли, файли повторної реєстрації, файли управління, файли трасування й файли дампів), будуть очищені до того, як вони будуть повторно використатися з метою, не пов'язаних з базою даних.

Наступна таблиця ілюструє, як кожна з вищезгаданих цілей протипоставлена загрозі, підтримує мета безпеки ОО, підтримує політикові або відображена в припущеннях про безпечне використання.

2.2.5 Основні функціональні вимоги безпеки

У наведеній нижче таблиці 2.4 перераховуються функціональні компоненти, включені в профіль захисту [2,7].

У класі ФВБ: аудит [class FAU: security AUdit] використовуються наступні розділи ФВБ

- реєстрація та облік подій;
- доступ до протоколу аудита;
- відбір подій для реєстрації й обліку;
- протокол аудита.

Таблиця 2.4 - Список функціональних компонентів

Компонент	Найменування
FAU_GEN.1	Генерація даних аудита
FAU_GEN.2	Асоціація ідентифікатора користувача
FAU_SAR.1	Перегляд аудита
FAU_SAR.3	Вибірковий перегляд аудита
FAU_SEL.1	Вибірний аудит
FAU_STG.1	Захищене зберігання журналу аудита
FAU_STG.4	Запобігання втрати даних аудита
FDP_ACC.1	Обмежене управління доступом
FDP_ACF.1	Управління доступом, засноване на атрибутах безпеки

Компонент	Найменування
FDP_RIP.2	Повний захист залишкової інформації
FIA_ATD.1	Визначення атрибутів користувача
FIA_UID.1	Вибір моменту ідентифікації
FIA_USB.1	Зв'язування користувач-суб'єкт
FMT_MSA.1	Управління атрибутами безпеки
FMT_MSA.3	Ініціалізація статичних атрибутів
FMT_MTD.1	Управління даними ФБО
FMT_REV.1	Скасування
FMT_SMR.1	Ролі безпеки
FPT_RVM.1	Неможливість обходу ПБО
FPT_SEP.1	Відділення домена ФБО
FRU_RSA.1	Максимальні квоти
FTA_MCS.1	Базове обмеження на паралельні сеанси
FTA_TSE.1	Відкриття сеансу з ОО

•

Розділ ФВБ: реєстрація й облік подій [security audit data GENeration (FAU_GEN)] використовуються незалежні функціональні вимоги безпеки:

• реєстрація заданої множини подій і задавання облікової інформації для подій кожного типу [audit data generation (FAU_GEN.l)];

• реєстрація, облік подій та реєстрація користувачів, які ініціювали події [user identity association (FAU_GEN.2)].

Розділ ФВБ: доступ до протоколу аудита [Security Audit Review (FAU_SAR)] використовуються незалежні функціональні вимоги безпеки:

• надання доступу до протоколу аудита для обмеженого набору авторизованих користувачів [audit review (FAU_SAR.l)];

• вибіркове керування доступом до протоколу аудита [selectable audit review (FAU_SAR.3)].

Розділ ФВБ: відбір подій для реєстрації та обліку [security audit event SELection (FAU_SEL)] включає вимогу безпеки — визначення множини властивих аудитові подій на основі заданого набору атрибутів [selective audit (FAU_SEL.l)].

Розділ ФВБ: протокол аудита [security audit event SToraGe (FAU_STG)] використовуються дві незалежні функціональні вимоги безпеки:

• виділення ресурсів під протокол аудита, захист протоколів від неавторизованої модифікації або видалення [protected audit trail storage (FAU_STG.l)];

• •попередження втрат записів аудита у випадку вичерпання ресурсів, які відведені під протокол аудита [prevention of audit data loss (FAU_STG.4)].

У класі ФВБ: захист інформації [class FDP: user Data Protection] використовуються наступні розділи ФВБ (рис. 5.14, 5.15):

• політики керування доступом;

• засоби керування доступом;

• знищення залишкової інформації;

Розділ ФВБ: політики керування доступом [ACcess Control policy (FDP_ACC) включає тільки вимогу безпеки - керування доступом для обмеженої множини операцій і об'єктів [subset access control (FDP_ACC.l)];

Розділ ФВБ: засоби керування доступом [Access Control Functions (FDP_ACF)] включає вимогу безпеки — керування доступом на основі атрибутів безпеки або іменованих груп атрибутів із явним дозволом або відмовою в доступі [security attribute based access control (FDP_ACF.l)].

Розділ ФВБ: знищення залишкової інформації [Residual Information Protection (FDP_RIP)] включає тільки вимогу безпеки - знищення залишкової інформації для всіх об'єктів при їх створенні або вилученні [full residual information protection (FDP_RIP.2)].

У класі ФВБ: ідентифікація і автентифікація [class FIA: Identification and Authentication] використовуються наступні розділи ФВБ:

- атрибути безпеки користувачів;
- ідентифікація користувачів;
- відповідність користувачів і суб'єктів.

Розділ ФВБ: атрибути безпеки користувачів [user ATtri-bute Definition (FIA_ATD)] включає вимогу безпеки — індивідуальне призначення атрибутів безпеки користувачів [user attribute definition **(FIA_ATD.l)].**

Розділ ФВБ: ідентифікація користувачів [User IDentifi-cation (FIA_UID)] включає тільки вимогу безпеки - обов'язковість ідентифікації користувачів [timing of identification (FIA_UID.l)];

Розділ ФВБ: відповідність користувачів і суб'єктів [User-Subject Binding (FIA_USB)] включає вимогу безпеки — присвоєння суб'єктам, що діють від імені користувача, його атрибутів безпеки [user-subject binding (FIA_USB.l)].

У класі ФВБ: управління безпекою [class FMT: security ManegemenT] використовуються наступні розділи ФВБ (рис. 5.17):

- управління атрибутами безпеки;
- управління параметрами та конфігурацією засобів захисту;
- відкликання атрибутів безпеки;
- адміністративні ролі.

3 ОСНОВНІ МЕТОДИ ТА ЗАСОБИ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

3.1 Автентифікація, авторизація й адміністрування дій користувачів

З кожним зареєстрованим у комп'ютерній системі суб'єктом (користувачем або процесом, що діє від імені користувача) зв'язана деяка інформація, що однозначно ідентифікує його. Це може бути число або рядок символів, що йменують даний суб'єкт. Цю інформацію називають *ідентифікатором* суб'єкта. Якщо користувач має ідентифікатор, зареєстрований у мережі, він уважається легальним (законним) користувачем; інші користувачі ставляться до нелегальних користувачів. Перш ніж одержати доступ до ресурсів комп'ютерної системи, користувач повинен пройти процес первинної взаємодії з комп'ютерною системою, що включає ідентифікацію й автентифікацію.

Ідентифікація (Identification) - це процедура розпізнавання користувача по його ідентифікаторі (імені). Ця функція виконується в першу чергу, коли користувач робить спробу ввійти в мережу. Користувач повідомляє системі по її запиті свій ідентифікатор, і система перевіряє у своїй базі даних його наявність.

Автентифікація (Authentication) - процедура перевірки дійсності заявленого користувача, процесу або пристрою. Ця перевірка дозволяє вірогідно переконатися, що користувач (процес або пристрій) є саме тим, ким себе повідомляє. При проведенні автентифікації сторона, що перевіряє, переконується в дійсності перевіряє сторони, що, при цьому перевіряє сторона, що, теж бере активну участь у процесі обміну інформацією. Звичайно користувач підтверджує свою ідентифікацію, уводячи в систему унікальну, не відому іншим користувачам інформацію про себе (наприклад, пароль або сертифікат).

Ідентифікація й автентифікація є взаємозалежними процесами розпізнавання й перевірки дійсності суб'єктів (користувачів). Саме від них залежить наступне рішення системи, чи можна дозволити доступ до ресурсів системи конкретному користувачеві або процесу. Після ідентифікації й автентифікації суб'єкта виконується його авторизація.

Авторизація (Authorization) - процедура надання суб'єктові певних повноважень і ресурсів у даній системі, іншими словами, авторизація встановлює сферу його дії й доступні йому ресурси. Якщо система не може надійно відрізнити авторизовану особу від неавторизованого, конфіденційність і цілісність інформації в цій системі можуть бути порушені. Із процедурами автентифікації й авторизації тісно зв'язана процедура адміністрування дій користувача.

Адміністрування (Accounting) - це реєстрація дій користувача в мережі, включаючи його спроби доступу до ресурсів. Хоча ця облікова інформація може бути використана для виписування рахунку, з позицій безпеки вона особливо важлива для виявлення, аналізу інцидентів безпеки в мережі й відповідному реагуванні на них. Запису в системному журналі, аудиторські перевірки й Поадміністрування - все це може бути використане для забезпечення підзвітності користувачів, якщо що-небудь трапиться при вході в мережу з їхнім ідентифікатором.

Необхідний рівень автентифікації визначається вимогами безпеки, які встановлені в організації. Загальнодоступні Web-сервери можуть дозволити анонімний або гостьовий доступ до інформації. Фінансові транзакції можуть зажадати строгої автентифікації. Прикладом слабкої форми автентифікації може служити використання IP-адреси для визначення користувача. Підміна (spoofing) IP-адреси може легко зруйнувати цей механізм автентифікації. Стругаючи автентифікація вимагає, принаймні, двухфакторной перевірки дійсності.

Авторизація визначає повноваження (privilege), надавані обслуговуючою програмою конкретній особі або групі осіб, по одержанню доступу до сервисам або інформації. У добре захищених системах не повинна допускатися авторизація за замовчуванням, а будь-які додаткові повноваження базуються на мінімальному привілеї й виходячи із прямих обов'язків користувача (need-to-know). У відкритих системах авторизація може бути надана гостеві або анонімним користувачам. Організації необхідно чітко визначити свої вимоги до безпеки, щоб ухвалювати рішення щодо відповідних границях авторизації.

Процедура авторизації базується на відносинах довіри. Процес надання доступу повинен довіряти процесу автентифікації особи (identity). Зловмисники можуть намагатися добути пароль авторизованого користувача, перехопити сесію Telnet або використати соціальну інженерію для підміни авторизованого користувача й одержання його прав доступу. Надійна автентифікація є тим ключовим фактором, що гарантує, що тільки авторизовані користувачі одержать доступ до контрольованої інформації.

При захисті каналів передачі даних повинна виконуватися *взаємна автентифікація суб'єктів,* тобто взаємне підтвердження дійсності суб'єктів, що зв'язуються між собою по лініях зв'язку. Процедура підтвердження дійсності виконується звичайно на початку сеансу в процесі встановлення з'єднання абонентів. Термін “з'єднання” указує на логічний зв'язок (потенційно двосторонню) між двома суб'єктами мережі. Ціль даної процедури - забезпечити впевненість, що з'єднання встановлене із законним суб'єктом і всією інформацією дійде до місця призначення.

Для підтвердження своєї дійсності суб'єкт може пред'являти системі різні сутності. Залежно від пропонованих суб'єктом сутностей процеси автентифікації можуть бути розділені на наступні категорії:

- *на основі знання чого-небудь.* Прикладами можуть служити пароль, персональний ідентифікаційний код PIN (Personal Identification Number), а також секретні й відкриті ключі, знання яких демонструється в протоколах типу “запит-відповідь”;
- *на основі володіння чим-небудь.* Звичайно це магнітні картки, смарт-картки, сертифікати й пристрої touch memory;
- *на основі яких-небудь невід'ємних характеристик.* Ця категорія включає методи, що базуються на перевірці біометричних характеристик користувача (голосу, райдужної оболонки й сітківки ока, відбитків пальців, геометрії долоні й ін.)* У даній категорії не використаються криптографічні методи й засоби. Автентифікація на основі біометричних характеристик застосовується для контролю доступу в приміщення або до якої-небудь техніки.

Пароль - це те, що знає користувач і що також знає інший учасник взаємодії. Для взаємної автентифікації учасників взаємодії може бути організований обмін паролями між ними. Персональний ідентифікаційний номер PIN є випробуваним способом автентифікації власника пластикової картки й смарт-картки. Секретне значення PIN-коду повинне бути відомо тільки власникові картки.

Динамічний (одноразовий) пароль - це пароль, що після однократного застосування ніколи більше не використається. На практиці звичайно використається регулярно мінливе значення, що базується на постійному паролі або ключовій фразі.

Система "запит-відповідь" - одна зі сторін ініціює автентифікацію за допомогою посилки іншій стороні унікального й непередбаченого значення "запит", а інша сторона посилає відповідь, обчислена за допомогою запиту й секрету. Тому що обидві сторони володіють одним секретом, те перша сторона може перевірити правильність відповіді другої сторони.

Сертифікати й цифрові підписи - якщо для автентифікації використаються сертифікати, то потрібне застосування й цифрові підписи на цих сертифікатах. Сертифікати видаються відповідальною особою в організації користувача, сервером сертифікатів або зовнішньою довіреною організацією. У рамках Internet з'явився ряд комерційних інфраструктур керування відкритими ключами PKI (Public Key Infrastructure) для поширення сертифікатів відкритих ключів. Користувачі можуть одержати сертифікати різних рівнів.

Процеси автентифікації можна також класифікувати за рівнем забезпечуваної безпеки. Відповідно до даного підходу процеси автентифікації розділяються на наступні типи:

- автентифікація, що використає паролі й цифрові сертифікати;
- стругаючи автентифікація на основі використання криптографічних методів і засобів;
- процеси (протоколи) автентифікації, що володіють властивістю доказу з нульовим знанням;
- біометрична автентифікація користувачів.

З погляду безпеки кожний з перерахованих типів сприяє рішенню своїх специфічних завдань, тому процеси й протоколи автентифікації активно використаються на практиці. У той же час слід зазначити, що інтерес до протоколів автентифікації, що володіють властивістю доказу з нульовим знанням носить поки скоріше теоретичний, ніж практичний характер, але, можливо, у недалекому майбутньому їх почнуть активно використати для захисту інформаційного обміну.

Основними атаками на протоколи автентифікації є:

- *маскарад* (impersonation). Користувач намагається видати себе за інший з метою одержання привілеїв і можливості дій від імені, цього користувача;
- *підміна сторони* автентифікаційного обміну (interleaving attack). Зловмисник у ході даної атаки бере участь у процесі автентифікаційного обміну між двома сторонами з метою модифікації минаючого через нього трафика. Іс-

нує різновид атаки підміни: після успішного проходження автентифікації між двома користувачами й установлення з'єднання порушник виключає якого-небудь користувача із з'єднання й продовжує роботу від його імені;

•*повторна передача* (replay attack). Полягає в повторній передачі автентифікаційних даних яким-небудь користувачем;

•*відбиття передачі* (reflection attack). Один з варіантів попередньої атаки, у ході якої зловмисник у рамках даної сесії протоколу пересилає назад перехоплену інформацію;

•*змушена затримка* (forced delay). Зловмисник перехоплює яку-небудь інформацію й передає її через деякий час;

•*атака з вибіркою тексту* (chosen-text attack). Зловмисник перехоплює автентифікаціонный трафик і намагається одержати інформацію про довгострокові криптографічні ключі.

Для запобігання таких атак при побудові протоколів автентифікації застосовуються наступні прийоми:

• використання механізмів типу “запит-відповідь”, міток часу, випадкових чисел, ідентифікаторів, цифрових підписів;

• прив'язка результату автентифікації до наступних дій користувачів у рамках системи. Прикладом подібного підходу може служити здійснення в процесі автентифікації обміну секретними сеансовыми ключами, які використаються при подальшій взаємодії користувачів;

• періодичне виконання процедур автентифікації в рамках уже встановленого сеансу зв'язку й т.п.

Механізм “запит-відповідь” полягає в наступному. Якщо користувач A хоче бути впевненим, що повідомлення, одержувані їм від користувача B, не є помилковими, він включає в, що посилає для B повідомлення непередбачений елемент - запит X (наприклад, деяке випадкове число). При відповіді користувач B повинен виконати над цим елементом певну операцію (наприклад, обчислити деяку функцію $f(X)$). Це неможливо здійснити заздалегідь, тому що користувачеві B не відомо, яке випадкове число X прийде в запиті. Одержавши відповідь із результатом дій B, користувач A може бути впевнений, що B - справжній. Недолік цього методу - можливість установлення закономірності між запитом і відповіддю.

Механізм оцінки часу має на увазі реєстрацію часу для кожного повідомлення. У цьому випадку кожен користувач мережі може визначити, наскільки застаріло повідомлення, що прийшло, і вирішити не приймати його, оскільки воно може бути помилковим.

В обох випадках для захисту механізму контролю варто застосовувати шифрування, щоб бути впевненим, що відповідь послана не зловмисником.

При використанні оцінок часу виникає проблема *припустимого тимчасового інтервалу затримки* для підтвердження дійсності сеансу. Адже повідомлення з “тимчасовим штемпелем”, у принципі, не може бути передане миттєво. Крім того, комп'ютерні годинники одержувача й відправника не можуть бути абсолютно синхронізовані.

При порівнянні й виборі протоколів автентифікації необхідно враховувати наступні характеристики:

•*наявність взаємної автентифікації.* Ця властивість відбиває необхідність обопільної автентифікації між сторонами автентифікаційного обміну;

•*обчислювальна ефективність.* Кількість операцій, необхідних для виконання протоколу;

•*комунікаційна ефективність.* Дана властивість відбиває кількість повідомлень й їхню довжину, необхідні для здійснення автентифікації;

•*наявність третьої сторони.* Прикладом третьої сторони може служити довірений сервер розподілу симетричних ключів або сервер, що реалізує дерево сертифікатів для розподілу відкритих ключів;

•*основа гарантій безпеки.* Прикладом можуть служити протоколи, що володіють властивістю доказу з нульовим знанням;

•*зберігання секрету.* Мається на увазі спосіб зберігання критичної ключової інформації.

3.2 Методи автентифікації, що використають паролі й цифрові сертифікати

Однієї з розповсюджених схем автентифікації є *проста автентифікація,* що заснована на застосуванні традиційних багаторазових паролів з одночасним узгодженням засобів його використання й обробки. Автентифікація на основі багаторазових паролів є простим і наочним прикладом використання поділюваної інформації. Поки в більшості видів захищених віртуальних мереж VPN (Virtual Private Network) доступ клієнта до сервера дозволяється по паролі. Однак все частіше застосовуються більш ефективні засоби автентифікації, наприклад програмні й апаратні системи автентифікації на основі одноразових паролів, цифрових сертифікатів.

3.2.1 Автентифікація на основі одноразових паролів

Базовий принцип “єдиного входу” припускає достатність одноразового проходження користувачем процедури автентифікації для доступу до всіх мережних ресурсів. Тому в сучасних операційних системах передбачається централізована служба автентифікації, що виконується одним із серверів мережі й використає для своєї роботи базу даних. У цій базі даних зберігаються облікові дані про користувачів мережі. У ці облікові дані поряд з іншою інформацією включені ідентифікатори й паролі користувачів. Процедуру простий автентифікації користувача в мережі можна представити в такий спосіб. При спробі логічного входу в мережу користувач набирає на клавіатурі комп'ютера свої ідентифікатор і пароль. Ці дані надходять для обробки на сервер автентифікації. У базі даних, що зберігається на сервері автентифікації, по ідентифікаторі користувача перебуває відповідний запис, з її витягається пароль і рівняється з тим паролем, що ввів користувач. Якщо вони збіглися, то автентифікація прой-

шла успішно, користувач одержує легальний статус і ті права й доступ до ресурсів мережі, які визначені для його статусу системою авторизації.

У схемі простий автентифікації передача пароля й ідентифікатора користувача може виконуватися такими способами:

- у незашифрованому виді; наприклад, відповідно до протоколу парольної автентифікації PAP (Password Authentication Protocol) паролі передаються по лінії зв'язку у відкритій незахищеній формі;
- у захищеному виді; всі передані дані (ідентифікатор і пароль користувача, випадкове число й мітки часу) захищені за допомогою шифрування або односпрямованої функції.

Схема простий автентифікації з використанням пароля показана на рисунку 3.1.

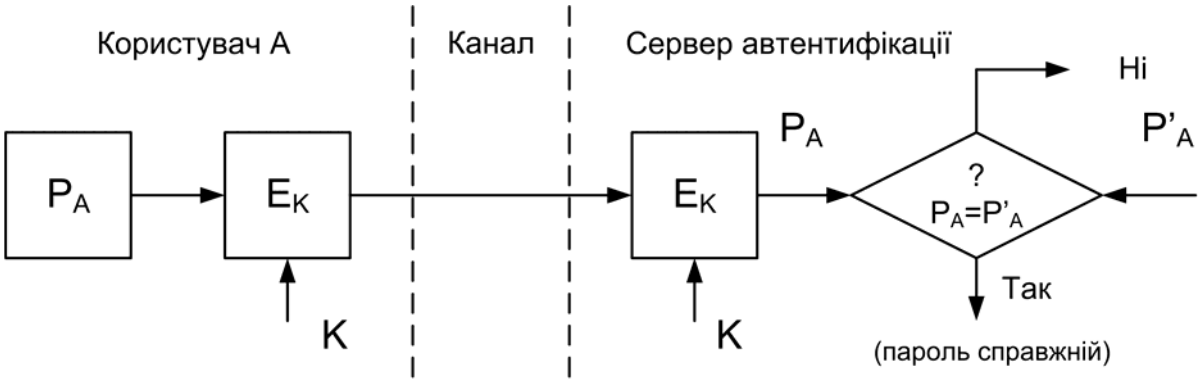

Рисунок 3.1 - Проста автентифікація з використанням пароля

Очевидно, що варіант автентифікації з передачею пароля користувача в незашифрованому виді не гарантує навіть мінімального рівня безпеки, тому що піддано численним атакам і легко компрометується. Щоб захистити пароль, його потрібно зашифрувати перед пересиланням по незахищеному каналі. Для цього в схему включені засоби шифрування E_K й расшифрования D_K, керовані поділюваним секретним ключем K. Перевірка дійсності користувача заснована на порівнянні присланого користувачем пароля P_A й вихідного значення $P_A^{'}$ хранящегося в сервері автентифікації. Якщо значення P_A й $P_A^{'}$ збігаються, то пароль P_A уважається справжнім, а користувач A - законним.

Схеми організації простий автентифікації відрізняються не тільки методами передачі паролів, але й видами їхнього зберігання й перевірки. Найпоширенішим способом є зберігання паролів користувачів у відкритому виді в системних файлах, причому на ці файли встановлюються атрибути захисту від читання й запису (наприклад, за допомогою опису відповідних привілеїв у списках контролю доступу операційної системи). Система зіставляє уведений користувачем пароль із записом, що зберігається у файлі паролів. При цьому способі не використаються криптографічні механізми, такі як шифрування або односпрямовані функції. Очевидним недоліком даного способу є можливість одер-

жання зловмисником у системі привілеїв адміністратора, включаючи права доступу до системних файлів й, зокрема, до файлу паролів.

З погляду безпеки більше кращим є метод передачі й зберігання паролів з використанням однобічних функцій. У цьому випадку користувач повинен пересилати замість відкритої форми пароля його відображення, одержуване з використанням однобічної функції h(.). Це перетворення гарантує неможливість розкриття супротивником пароля по його відображенню, тому що супротивник натрапляє на нерозв'язне числове завдання.

Наприклад, однобічна функція $h(.)$ може бути визначена в такий спосіб:

$$h(P) = E_P(ID),$$

де P - пароль користувача,

ID - ідентифікатор користувача,

E_P - процедура шифрування, виконувана з використанням пароля P як ключ. Такі функції зручні, якщо довжина пароля й ключа однакові. У цьому випадку перевірка дійсності користувача A за допомогою пароля P_A складається з пересилання серверу автентифікації відображення $h(P_A)$ й порівняння його з попередньо обчисленим і збереженим у базі даних сервера автентифікації еквівалентом $h'(P_A)$ як показане на рисунку 4.2. Якщо відображення $h(P_A)$ й $h'(P_A)$ рівні, то вважається, що користувач успішно пройшов автентифікацію.

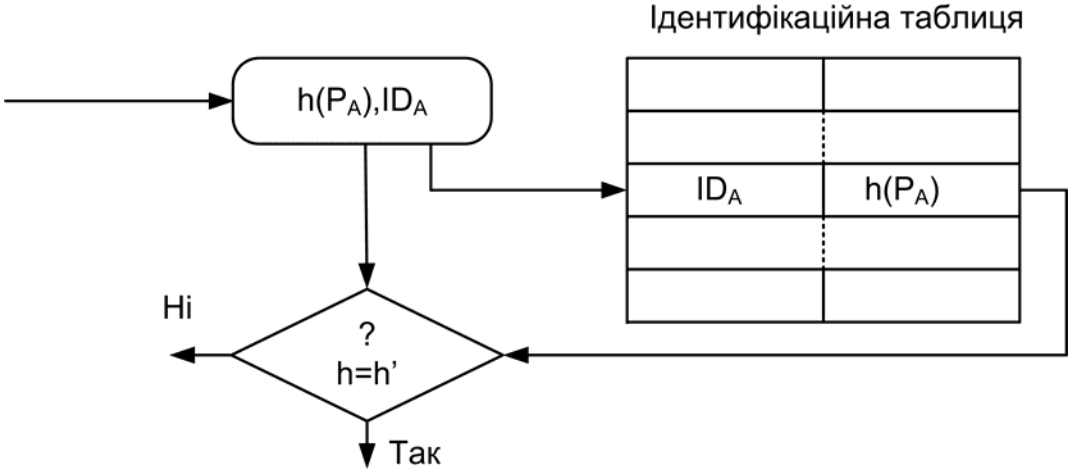

Рисунок 4.2 - Використання однобічної функції для перевірки пароля

На практиці паролі складаються лише з декількох символів, щоб дати можливість користувачам запам'ятати їх. Короткі паролі уразливі до атаки повного перебору всіх варіантів. Для того щоб запобігти такій атаці, функцію $h(P_A)$ можна визначити інакше, наприклад у вигляді:

$$h(P) = E_P E_K(ID),$$

де K й ID - відповідно ключ й ідентифікатор відправника.

Розрізняють дві форми подання об'єктів, що автентифікують користувача:

- зовнішній автентифікуючий об'єкт, що не належить системі;

• внутрішній об'єкт, що належить системі, у який переноситься інформація із зовнішнього об'єкта.

Зовнішні об'єкти можуть бути представлені на різних носіях інформації - пластикових картках, смарт-картках, гнучких магнітних дисках і т.п. Природно, що зовнішня й внутрішня форми подання автетифікуючого об'єкта повинні бути семантично тотожні.

Допустимо, що в комп'ютерній системі зареєстровано п користувачів. Нехай i-й автентифікуючий об'єкт i-го користувача містить два інформаційні поля:

ID_j - незмінний ідентифікатор і-го користувача, що є аналогом імені й використається для ідентифікації користувача;

K_j - автентифікуюча інформація користувача, що може змінюватися й використається для автентифікації (наприклад, пароль $P_i = K_i$).

Описана структура відповідає практично будь-якому ключовому носію інформації, використовуваному для впізнання користувача. Наприклад, для носіїв типу пластикових карток виділяється незмінна інформація ID; первинної персонализации користувача й об'єкт у файловій структурі картки, що містить K_j.

Сукупну інформацію в ключовому носії можна назвати первинної автентифікуючою інформацією i-го користувача. Очевидно, що внутрішній автетифікуючий об'єкт не повинен існувати в системі тривалий час (більше часу роботи конкретного користувача). Для тривалого зберігання варто використати дані в захищеній формі.

Розглянемо дві типові схеми ідентифікації й автентифікації.

Схема 1. У комп'ютерній системі виділяється об'єкт-еталон для ідентифікації й автентифікації користувачів. Структура об'єкта-еталона для схеми 1 показана в таблиці 4.1.

Таблиця 4.1

Номер користувача	Інформація для ідентифікації	Інформація автентифікації
1	ID_1	E_1
2	ID_2	E_2
...	…	…
N	ID_n	E_n

Тут $E_i = F(ID_i, K_i)$, де F - функція, що має властивість “невідновності” значення K_i по E_i й ID. “Невідновність” K_i оцінюється деякою граничною трудомісткістю T_υ рішення завдання відновлення автентифікуючої інформації K_i ,по E_i й ID. Крім того, для пари K_i й K_j можливий збіг відповідних значень E. У зв'язку із цим імовірність помилкової автентифікації користувача не

повинна бути більше деякого граничного значення P_0. На практиці задають значення $T_\upsilon == 10^{20} - 10^{30}$, $P_\upsilon = 10^{-7} - 10^{-9}$.

Протокол ідентифікації й автентифікації (для схеми 1):

1. Користувач пред'являє системі свій ідентифікатор ID.
2. Система звіряє пред'явлений ID із зареєстрованими $ID_i, i = 1 - n$. Якщо ID не збігається з жодним ID_i, зареєстрованим у системі, то ідентифікація відкидається - користувач не допускається до роботи. Якщо $ID - ID_i$, то вважається, що користувач, що назвався користувачем i, пройшов ідентифікацію.
3. Система запитує в користувача його автентифікатор.
4. Користувач пред'являє системі автентифікатор K.
5. Система обчислює значення $Y = F(ID_i, K)$ й порівнює значення Y й E_i.

При збігу цих значень установлюється, що даний користувач успішно пройшов автентифікацію в системі. Інформація про цього користувача передається в програмні модулі, що використають ключі користувачів (тобто в систему шифрування, розмежування доступу й ін.). У противному випадку автентифікація відкидається - користувач не допускається до роботи.

Дана схема ідентифікації й автентифікації користувача може бути модифікована.

Схема 2. У комп'ютерній системі виділяється модифікований об'єкт-еталон, структура якого показана в таблиці 4.2.

Таблиця 4.2

Номер користувача	Інформація для ідентифікації	Інформація автентифікації
1	ID_1,S_1	E_1
2	ID_2,S_2	E_2
...	…	…
N	ID_n,S_n	E_n

На відміну від схеми 1, у схемі 2 значення $E_i = F(S_i, K_i)$, де S_i - випадковий вектор, що задає при створенні ідентифікатора користувача, тобто при створенні рядка, необхідної для ідентифікації й автентифікації користувача; F - функція, що має властивість "невідновності" значення K по E_i й S_i.

Протокол ідентифікації й автентифікації (для схеми 2):

1. Користувач пред'являє системі свій ідентифікатор ID.
2. Якщо ID не збігається з жодним ID_i, зареєстрованим у комп'ютерній системі, то ідентифікація відкидається - користувач не допускається до роботи.

Если існує $ID_i = ID$, тоді встановлюється, що користувач, що назвався користувачем i, пройшов ідентифікацію.

3. По ідентифікаторі ID виділяється вектор S_i.
4. Система запитує в користувача автентифікатор.
5. Користувач пред'являє системі автентифікатор K.
6. Система обчислює значення $Y = F(S_i, K)$ й порівнює значення S й E_i.

При збігу цих значень установлюється, що даний користувач успішно пройшов автентифікацію в системі. У противному випадку автентифікація відкидається, і користувач не допускається до роботи.

Друга схема автентифікації застосовується в операційній системі UNIX. Як ідентифікатор ID використається ім'я користувача (запитане по Login), у якості автентифікатора K_i - пароль користувача (запитаний по Password), функція F являє собою алгоритм шифрування DES. Еталони для ідентифікації й автентифікації втримуються у файлі Etc/passwd.

Системи простої автентифікації на основі багаторазових паролів мають знижену стійкість, оскільки в них вибір автентифікуючої інформації відбувається із відносно невеликої безлічі осмислених слів. Термін дії багаторазового пароля повинен бути визначений у політику безпеки організації, і такі паролі повинні регулярно змінюватися. Вибирати паролі потрібно так, щоб вони були важкі для вгадування й не були присутні в словнику.

3.2.2 Автентифікація на основі одноразових паролів

Схеми автентифікації, засновані на традиційних багаторазових паролях, не мають достатню безпеку. Такі паролі можна перехопити, розгадати, підглянути або украсти. Процедури автентифікації на основі одноразових паролів більше надійні.

Суть схеми одноразових паролів - використання різних паролів при кожному новому запиті на надання доступу. Одноразовий динамічний пароль дійсний тільки для одного входу в систему. Навіть якщо хтось перехопив його, пароль виявиться марний. Динамічний механізм завдання пароля є одним із кращих способів захистити процес автентифікації від погроз ззовні. Як правило, системи автентифікації з одноразовими паролями використаються для перевірки вилучених користувачів.

Відомі наступні методи застосування одноразових паролів для автентифікації користувачів:

1. Використання механізму тимчасових міток на основі системи єдиного часу.
2. Використання загального для легального користувача й списку, що перевіряє, випадкових паролів і надійного механізму їхньої синхронізації.
3. Використання загального для користувача й генератора, що перевіряє, псевдовипадкових чисел з тим самим початковим значенням.

Генерація одноразових паролів може здійснюватися апаратним або програмним способом. Деякі апаратні засоби доступу на основі одноразових паролів реалізуються у вигляді мініатюрних пристроїв з убудованим мікропроцесором, зовні схожих на платіжні пластикові картки. Такі карти, звичайно називані ключами, можуть мати клавіатуру й невелике дисплейне вікно.

Як приклад реалізації першого методу розглянемо технологію автентифікації Securl на основі одноразових паролів з використанням апаратних ключів і механізму тимчасової синхронізації. Ця технологія автентифікації розроблена

компанією Security Dynamics і реалізована в комунікаційних серверах ряду компаній, зокрема в серверах компанії Cisco Systems й ін.

Схема автентифікації з використанням тимчасової синхронізації базується на алгоритмі генерації випадкових чисел через певний інтервал часу. Цей інтервал установлюється й може бути змінений адміністратором мережі. Схема автентифікації використає два параметри:

- секретний ключ, що представляє собою унікальне 64-бітове число, призначуване кожному користувачеві й даних автентифікаційного сервера, що зберігається в базі, і в апаратному ключі користувача;
- значення поточного часу.

Коли вилучений користувач робить спробу логічного входу в мережу, йому пропонується ввести його персональний ідентифікаційний номер PIN, що складається із чотирьох десяткових цифр, а також шість цифр випадкового числа, відображуваного в цей момент на дисплеї апаратного ключа. Використовуючи уведений користувачем PIN-код, сервер витягає з бази даних секретний ключ користувача й виконує алгоритм генерації випадкового числа, використовуючи як параметри витягнутий секретний ключ і значення поточного часу. Потім сервер перевіряє, чи збігаються згенероване сервер дозволяє користувачеві здійснити логічний вхід у систему.

При використанні цієї схеми автентифікації, природно, потрібно тверда тимчасова синхронізація апаратного ключа й сервера. Оскільки апаратний ключ може працювати кілька років, цілком можливо поступова неузгодженість внутрішніх годин сервера й апаратного ключа. Для рішення цієї проблеми компанія Security Dynamics застосовує два способи:

- при виробництві апаратного ключа точно виміряється відхилення частоти його таймера від номіналу. Величина цього відхилення враховується як параметр алгоритму сервера;
- сервер відслідковує коди, що генеруються конкретним апаратним ключем, і при необхідності динамічно підбудовується під цей ключ.

Зі схемою автентифікації, заснованої на тимчасовій синхронізації, зв'язана ще одна проблема. Генероване апаратним ключем випадкове число є достовірним паролем протягом невеликого кінцевого проміжку часу. Тому, у принципі, можлива короткочасна ситуація, коли зловмисник може перехопити PIN-код і випадкове число, щоб використати їх для доступу в мережу. Це саме уразливе місце схеми автентифікації, заснованої на тимчасовій синхронізації.

Існують й інші варіанти апаратної реалізації процедури автентифікації з використанням одноразових паролів, наприклад, автентифікація за схемою “запит-відповідь”. При спробі користувача здійснити логічний вхід у мережу автентифікаційний сервер передає йому запит у вигляді випадкового числа. Апаратний ключ користувача зашифровує це випадкове число, використовуючи, наприклад, алгоритм DES і секретний ключ користувача, що зберігається в пам'яті апаратного ключа й у базі даних сервера. Випадкове число-запит повертається в зашифрованому виді на сервер. Сервер, у свою чергу, також зашифровує згенероване ним самим випадкове число за допомогою того ж алгоритму DES і того ж секретного ключа користувача, витягнутого з бази даних сервера.

Потім сервер порівнює результат свого шифрування із числом, що прийшло від апаратного ключа. При збігу цих чисел користувач одержує дозвіл на вхід у мережу. Слід зазначити, що схема автентифікації “запит-відповідь” складніше у використанні в порівнянні зі схемою автентифікації з тимчасовою синхронізацією.

Другий метод застосування одноразових паролів для автентифікації користувачів заснований на вживанні загального для користувача й списку, що перевіряє, випадкових паролів і надійного механізму їхньої синхронізації. Поділюваний список одноразових паролів представляється у вигляді послідовності або набору секретних паролів, де кожен пароль уживається тільки один раз. Даний список повинен бути заздалегідь розподілений між сторонами автентифікаціонного обміну. Варіантом даного методу є використання таблиці запитів-відповідей, у якій утримуються запити й відповіді, уживані сторонами для проведення автентифікації, причому кожна пара повинна застосовуватися тільки один раз.

Третій метод застосування одноразових паролів для автентифікації користувачів заснований на вживанні загального для користувача й генератора, що перевіряє, псевдовипадкових чисел з тим самим початковим значенням. Відомі наступні варіанти реалізації цього методу:

- *послідовність преутворених одноразових паролів.* У ході чергової сесії автентифікації користувач створює й передає пароль саме для даної сесії, зашифрований на секретному ключі, отриманому з пароля попередньої сесії;
- *послідовності паролів, засновані на однобічній функції.* Суть даного методу становить послідовне використання однобічної функції (відома схема Лампорта). Цей метод є більше кращим з погляду безпеки в порівнянні з методом послідовно переутворених паролів.

Одним з найпоширеніших протоколів автентифікації на основі одноразових паролів є стандартизований в Internet протокол S/Key (RFC 1760). Даний протокол реалізований у багатьох системах, що вимагає перевірки дійсності вилучених користувачів, зокрема в системі TACACS+ компанії Cisco.

3.2.3 Автентифікація на основі сертифікатів

Коли число користувачів у мережі виміряється мільйонами, процедура попередньої реєстрації користувачів, пов'язана із призначенням і зберіганням паролів користувачів, стає вкрай громіздкої й практично погано реалізованою. У таких умовах автентифікація на основі цифрових сертифікатів є раціональною альтернативою застосуванню паролів.

При використанні цифрових сертифікатів комп'ютерна мережа, що дає доступ до своїх ресурсів, не зберігає ніякої інформації про своїх користувачів. Цю інформацію користувачі надають самі у своїх запитах-сертифікатах. Таке рішення масштабується набагато легше, ніж варіант із використанням паролів централізованою базою даних. При цьому завдання зберігання секретної інформації, зокрема закритих ключів, покладає тепер на самих користувачів.

Цифрові сертифікати, що засвідчують особистість користувача, видаються по запитах користувачів спеціальними вповноваженими організаціями - центрами сертифікації СА (Certificate Authority) - при виконанні певних умов. Слід зазначити, що сама процедура одержання сертифіката також включає етап перевірки дійсності (тобто автентифікації) користувача. Тут як проверяющей сторона виступає організація, що сертифікує (центр сертифікації СА).

Для одержання сертифіката клієнт повинен представити в центр сертифікації СА відомості, що засвідчують його особистість, і свій відкритий ключ. Перелік необхідних даних залежить від типу одержуваного сертифіката. організація, Що Сертифікує, після перевірки доказів дійсності користувача поміщає свій цифровий підпис у файл, що містить відкритий ключ і відомості про користувача, і видає сертифікат користувачеві, підтверджуючи факт приналежності даного відкритого ключа конкретній особі.

Сертифікат являє собою електронну форму, у якій утримується наступна інформація:

- відкритий ключ власника даного сертифіката;
- відомості про власника сертифіката, наприклад ім'я, адреса електронної пошти, найменування організації, у якій він працює, і т.п.;
- найменування організації, що сертифікує, що видала даний сертифікат;
- електронний підпис організації, що сертифікує, - зашифровані закритим ключем цієї організації дані, що втримуються в сертифікаті.

Сертифікат є засобом автентифікації користувача при його звертанні до мережних ресурсів. При цьому роль сторони, що перевіряє, грають сервери автентифікації корпоративної мережі. Сертифікати можна використати не тільки для автентифікації, але й для надання певних прав доступу. Для цього в сертифікат уводяться додаткові поля, у яких указується приналежність його власника тієї або іншої категорії користувачів.

Слід особливо зазначити тісний зв'язок відкритих ключів із сертифікатами. Сертифікат є не тільки посвідченням особи, але й посвідченням приналежності відкритого ключа. Цифровий сертифікат установлює й гарантує відповідність між відкритим ключем і його власником. Це запобігає погрозі підміни відкритого ключа.

Якщо абонент одержує від партнера по інформаційному обміні відкритий ключ у складі сертифіката, то він може перевірити цифровий підпис СА на цьому сертифікаті за допомогою відкритого ключа даного СА й переконатися, що отриманий відкритий ключ належить саме тому користувачеві, адреса й інші відомості про яке втримуються в даному сертифікаті. При використанні сертифікатів зникає необхідність зберігати на серверах корпорацій списки користувачів з їхніми паролями. На сервері досить мати список імен і відкритих ключів організацій, що сертифікують.

Застосування сертифікатів засноване на припущенні, що організацій, що сертифікують, відносно небагато і їхні відкриті ключі можуть бути доступні всім зацікавленим особам й організаціям (наприклад, за допомогою публікацій у журналах).

При реалізації процесу автентифікації на основі сертифікатів важливим є рішення питання про те, хто буде виконувати функції організації, що сертифікує. Цілком природним є рішення, при якому завдання забезпечення своїх співробітників сертифікатами бере на себе саме підприємство. Підприємство досить гарне інформовано про своїх співробітників і може взяти на себе завдання підтвердження їхньої особистості. Це спрощує процедуру первинної автентифікації при видачі сертифіката. Підприємства можуть використати існуючі програмні продукти, що забезпечують автоматизацію процесів генерації, видачі й обслуговування сертифікатів. Наприклад, компанія Netscape Communications пропонує свої сервери підприємствам для випуску ними власних сертифікатів.

Альтернативним рішенням для проблеми виконання функцій організації, що сертифікує, є залучення на комерційній основі незалежних центрів по видачі сертифікатів. Такі послуги пропонує, зокрема, що сертифікує центр компанії Verisign. Сертифікати компанії Verisign задовольняють вимогам міжнародного стандарту X.509. Ці сертифікати використаються в ряді продуктів захисту даних, наприклад у протоколі захищеного каналу SSL.

3.3 Строга автентифікація

3.3.1 Основні поняття

Ідея строгої автентифікації, реалізована в криптографічних протоколах, полягає в наступному. Сторона, яку перевіряють, доводить свою дійсність стороні, що перевіряє, демонструючи знання деякого секрету. Наприклад, цей секрет може бути попередньо розподілений безпечним способом між сторонами автентифікаційного обміну. Доказ знання секрету здійснюється за допомогою послідовності запитів і відповідей з використанням криптографічних методів і засобів.

Істотним є той факт, що сторона, що доводить, демонструє тільки знання секрету, але сам секрет у ході автентифікаційного обміну не розкривається. Це забезпечується за допомогою відповідей сторони, що доводить, на різні запити сторони, що перевіряє. При цьому результуючий запит залежить тільки від користувальницького секрету й початкового запиту, що звичайно представляє довільно обране на початку протоколу велике число.

У більшості випадків стругаючи автентифікація полягає в тім, що кожен користувач автентифікується за ознакою володіння своїм секретним ключем. Інакше кажучи, користувач має можливість визначити, чи володіє його партнер по зв'язку належним секретним ключем і чи може він використати цей ключ для підтвердження того, що дійсно є справжнім партнером по інформаційному обміні.

Відповідно до рекомендацій стандарту X.509 розрізняють процедури строгої автентифікації наступних типів:

- однобічна автентифікація;
- двостороння автентифікація;
- тристороння автентифікація.

Однобічна автентифікація передбачає обмін інформацією тільки в одному напрямку. Даний тип автентифікації дозволяє:

- підтвердити дійсність тільки однієї сторони інформаційного обміну;
- виявити порушення цілісності переданої інформації;
- виявити проведення атаки типу “повтор передачі”;
- гарантувати, що переданими автентифікаційними даними може скористатися тільки сторона, що перевіряє.

Двостороння автентифікація в порівнянні з однобічної містить додаткова відповідь сторони, що перевіряє, що доводить стороні. Ця відповідь повинен переконати сторону, що перевіряє, що зв'язок установлюється саме з тією стороною, який були призначені автентифікаціонные дані.

Трехсторонняя автентифікація містить додаткову передачу даних від сторони, що доводить, що перевіряє. Цей підхід дозволяє відмовитися від використання міток часу при проведенні автентифікації.

Слід зазначити, що дана класифікація досить умовна. Відзначені особливості носять більшою мірою теоретичний характер. На практиці набір використовуваних прийомів і засобів залежить безпосередньо від конкретних умов реалізації процесу автентифікації. Необхідно також ураховувати, що проведення строгої автентифікації вимагає обов'язкового узгодження сторонами використовуваних криптографічних алгоритмів і ряду додаткових параметрів.

Перш ніж перейти до розгляду конкретних варіантів протоколів строгої автентифікації, варто зупинитися на призначенні й можливостях так званих одноразових параметрів, використовуваних у протоколах автентифікації. Ці одноразові параметри іноді називають *nonces*. По визначенню, *nonci* - це величина, використовувана для однієї й тієї ж мети не більше одного разу.

Серед використовуваних на сьогоднішній день одноразових параметрів варто виділити: випадкові числа, мітки часу й номери послідовностей.

Одноразові параметри дозволяють уникнути повтору передачі, підміни сторони автентифікаціонного обміну й атаки з вибором відкритого тексту. За допомогою одноразових параметрів можна забезпечити унікальність, однозначність і тимчасові гарантії переданих повідомлень. Різні типи одноразових параметрів можуть як уживатися окремо, так і доповнювати один одного.

Можна привести наступні приклади застосування одноразових параметрів:

- перевірка своєчасності в протоколах, побудованих за принципом “запит-відповідь”. При такій перевірці можуть використатися випадкові числа, мітки часу із синхронізацією годин або номера послідовностей для конкретної пари (перевіряючий, що доводить);
- забезпечення своєчасності або гарантій унікальності. Здійснюється шляхом безпосереднього контролю одноразових параметрів протоколу (шляхом вибору випадкового числа) або побічно (за допомогою аналізу інформації, що втримується в поділюваному секреті);
- однозначна ідентифікація повідомлення або послідовності повідомлень. Здійснюється за допомогою вироблення одноразового значення з монотонно

зростаючої послідовності (наприклад, послідовності серійних номерів або міток часу) або випадкових чисел відповідної довжини.

Слід зазначити, що одноразові параметри широко використаються й в інших варіантах криптографічних протоколів (наприклад, у протоколах розподілу ключової інформації).

Залежно від використовуваних криптографічних алгоритмів протоколи строгої автентифікації можна розділити на наступні групи:

- протоколи строгої автентифікації на основі симетричних алгоритмів шифрування;
- протоколи строгої автентифікації на основі односпрямованих ключових хеш-функцій;
- протоколи строгої автентифікації на основі асиметричних алгоритмів шифрування;
- протоколи строгої автентифікації на основі алгоритмів електронного цифрового підпису.

3.3.2 Строга автентифікация, заснована на симетричних алгоритмах. Протокол Kerberos

Для роботи протоколів автентифікації, побудованих на основі симетричних алгоритмів, необхідно, щоб що перевіряє й доводить із самого початку мали той самий секретний ключ. Для закритих систем з невеликою кількістю користувачів кожна пара користувачів може заздалегідь розділити його між собою. У більших розподілених системах, що застосовують технологію симетричного шифрування, часто використаються протоколи автентифікації за участю довіреного сервера, з яким кожна сторона розділяє знання ключа. Такий сервер розподіляє сеансові ключі для кожної пари користувачів щораз, коли один з них запитує автентифікацію іншого. Гадана простота даного підходу є оманної, насправді розробка протоколів автентифікації цього типу є складною й з погляду безпеки не очевидної.

Протоколи автентифікації із симетричними алгоритмами шифрування

Нижче приводяться три приклади окремих протоколів автентифікації, специфікованих в ISO/IE З 9798-2. Ці протоколи припускають попередній розподіл поділюваних секретних ключів. Розглянемо наступні варіанти автентифікації:

- однобічна автентифікація з використанням міток часу;
- однобічна автентифікація з використанням випадкових чисел;
- двостороння автентифікація.

У кожному із цих випадків користувач доводить свою дійсність, демонструючи знання секретного ключа, тому що виконує расшифрование запитів за допомогою цього секретного ключа.

При використанні в процесі автентифікації симетричного шифрування необхідно також реалізувати механізми забезпечення цілісності переданих даних на основі загальноприйнятих способів.

Уведемо наступні позначення:

- r_A - випадкове число, згенероване учасником A;
- r_B - випадкове число, згенероване учасником B;
- t_A - мітка часу, згенерована учасником A;
- E_K - симетричне шифрування на ключі K (ключ K повинен бути попередньо розподілений між A й B).

Однобічна автентифікація, заснована на мітках часу:

$$A \to B : E_K(t_A, B) \quad (1)$$

Після одержання й расшифування даного повідомлення учасник B переконується в тім, що мітка часу t_A дійсна й ідентифікатор B, зазначений у повідомленні, збігається з його власним. Запобігання повторної передачі даного повідомлення ґрунтується на тім, що без знання ключа неможливо змінити мітку часу t_A й ідентифікатор B.

Однобічна автентифікація, заснована на використанні випадкових чисел:

$$A \leftarrow B : r_B \quad (1)$$

$$A \to B : E_K(r_B, B) \quad (2)$$

Учасник B відправляє учасникові A випадкове число r_B. Учасник A шифрує повідомлення, що складається з отриманого числа $г_в$ й ідентифікатора B, і відправляє зашифроване повідомлення учасникові B. Учасник B розшифровує отримане повідомлення й порівнює випадкове число, що втримується в повідомленні, з тим, що він послав учасникові A, Додатково він перевіряє ім'я, зазначене в повідомленні.

Двостороння автентифікація, що використає випадкові значення:

$$A \leftarrow B : r_B \quad (1)$$

$$A \to B : E_K(r_A, r_B, B) \quad (2)$$

$$A \leftarrow B : E_K(r_A, r_B) \quad (3)$$

При одержанні другого повідомлення учасник B виконує ті ж перевірки, що й у попередньому протоколі, і додатково розшифровує випадкове число r_A для включення його в третє повідомлення для учасника A. Третє повідомлення, отримане учасником A, дозволяє йому переконатися на основі перевірки значень r_A й r_B, що він має справу саме з учасником B.

Широко відомими представниками протоколів, що забезпечують автентифікацію користувачів із залученням у процесі автентифікації третьої сторони, є протокол розподілу секретних ключів Нідхема й Шредера й протокол Kerberos.

Протокол Kerberos

При розподілі ключів між учасниками майбутнього інформаційного обміну повинна бути гарантована дійсність сеансу зв'язку. Взаємне встановлення дійсності партнерів по обміні гарантує виклик потрібного суб'єкта з високим ступенем упевненості, що зв'язок установлений з необхідним адресатом і ніякими спробами підміни не був. Реальна процедура організації з'єднання між учасниками інформаційного обміну включає як етап підтвердження дійсності партнерів, так й етап властиво розподілу ключів.

Етап підтвердження дійсності учасників - це обмін повідомленнями, що засвідчують, щоб мати можливість виявити будь-яку підміну або повтор одного з попередніх викликів.

При включенні в процес *центра розподілу ключів KDC* (Key Distribution Center) здійснюється його взаємодія з одним або обома учасниками сеансу з метою розподілу секретних або відкритих ключів, призначених для використання в наступних сеансах зв'язку.

Розглянемо як приклад протокол автентифікації й розподілу секретних ключів Kerberos,

Протокол Kerberos використається для автентифікації в системах “клієнт-сервер” й обміну ключовою інформацією, призначеної для встановлення захищеного каналу зв'язку між абонентами, що працюють як у локальної, так й у глобальних мережах. Особливий інтерес даний протокол представляє тому, що він убудований як основний протокол автентифікації в операційній системі Microsoft Windows 2000 й UNIX BSD.

Kerberos забезпечує автентифікацію в мережах, що не заслуговують довіри, тобто при роботі Kerberos мається на увазі, що зловмисники можуть виконувати наступні дії:

- видавати себе за одну з легітимних сторін мережного з'єднання;
- мати фізичний доступ до одному з комп'ютерів, що беруть участь у з'єднанні;
- перехоплювати будь-які пакети, модифікувати їх й/або передавати повторно.

Відповідно, забезпечення безпеки в Kerberos побудовано таким чином, щоб нейтралізувати будь-які потенційні проблеми, які можуть виникнути через перерахованих вище дії зловмисників.

Створення Kerberos велося в рамках проекту Athena у Массачусетском технологічному університеті в середині 80-х років, і з тих пор цей протокол перетерпів ряд принципових змін, які відбилися в існуючим нині п'ятьох версіях.

Kerberos розроблений для мереж TCP/IP і побудований на основі довіри учасників протоколу до третього (довіреної) стороні. Служба Kerberos, що працює в мережі, діє як довірений посередник, забезпечуючи надійну автентифікацію в мережі з наступною авторизацією доступу клієнта (клієнтського додатка) до ресурсів мережі. Захищеність установлених у рамках сесії Kerberos з'єднань обумовлюється застосуванням симетричних алгоритмів шифрування. Служба Kerberos розділяє окремий секретний ключ із кожним суб'єктом мережі, і знання такого секретного ключа рівносильно доказу дійсності суб'єкта мережі.

Основу Kerberos становить протокол автентифікації й розподілу ключів Нідхема-Шредера (Needham-Schroeder) із третьою довіреною стороною. Розглянемо цю версію протоколу Нідхема-Шредера стосовно до Kerberos. У протоколі Kerberos (версія 5) беруть участь дві взаємодіючі сторони й довірений сервер KS, що виконує роль центра розподілу ключів KDC.

Зухвалий (вихідний) об'єкт позначається через A, а викликуваний (об'єкт призначення) - через B. Учасники сеансу A й B мають унікальні ідентифікатори Id_A й Id_B відповідно. Сторони A й B, кожна окремо, розділяють свій секретний ключ із сервером KS.

Нехай сторона A хоче одержати сеансовий ключ для інформаційного обміну зі стороною B.

Сторона A ініціює фазу розподілу ключів, посилаючи по мережі серверу KS ідентифікатори Id_A й Id_B:

$$A \to RS : Id_A, Id_B \qquad (l)$$

Сервер KS генерує повідомлення з тимчасовою оцінкою T, терміном дії L, випадковим сеансовим ключем K й ідентифікатором Id_A. Він шифрує це повідомлення секретним ключем, що розділяє зі стороною B.

Потім сервер KS бере тимчасову оцінку T, термін дії L, сеансовый ключ K, ідентифікатор Id_B сторони B й шифрує все це секретним ключем, що розділяє зі стороною A. Обоє ці зашифровані повідомлення він відправляє стороні A:

$$KS \to A : E_A(T, L, Id_B), E_B(T, L, Id_A) \qquad (2)$$

Сторона A розшифровує перше повідомлення своїм секретним ключем, перевіряє оцінку часу T, щоб переконатися, що це повідомлення не є повторенням попередньої процедури розподілу ключів. Потім сторона A генерує повідомлення зі своїм ідентифікатором Id_A й оцінкою часу T, шифрує його сеансовим ключем K і відправляє стороні B. Крім того, A відправляє для B повідомлення від KS, зашифроване ключем сторони B:

$$A \to B : E_K(Id_A, T), E_B(T, L, K, Id_A)$$

(3)

Тільки сторона B може розшифрувати повідомлення (3). Сторона B одержує оцінку часу T, термін дії L, сеансовий ключ K й ідентифікатор Id_A. Потім сторона B розшифровує сеансовим ключем K другу частину повідомлення (3). Збіг значень T й Id_A у двох частинах повідомлення підтверджують дійсність A по відношенню к. B

Для взаємного підтвердження дійсності сторона B створює повідомлення, що складається з оцінки часу T плюс 1, шифрує його ключем K і відправляє стороні A:

$$B \to A : E_K(T + 1) \qquad (4)$$

Якщо після розшифрування повідомлення (4) сторона A одержує очікуваний результат, вона знає, що на іншому кінці лінії зв'язку перебуває дійсно B.

Цей протокол успішно працює за умови, що годинники кожного учасника синхронізовані з годинниками сервера KS. Слід зазначити, що в цьому протоколі необхідний обмін із KS для одержання сеансового ключа щораз, коли A бажає встановити зв'язок с. B Протокол забезпечує надійне з'єднання об'єктів A і B за умови, що жоден із ключів не скомпрометований і сервер KS захищений.

Система Kerberos має структуру типу “клієнт-сервер” і складається із клієнтських частин C, установлених на всі машини мережі (робітники станції користувачів і сервери), і сервера Kerberos KS, що розташовується на якому-небудь (не обов'язково виділеному) комп'ютері. Клієнтами можуть бути користувачі, а також незалежні програми, що виконують такі дії, як завантаження вилучених файлів, відправлення повідомлень, доступ до баз даних, доступ до принтерів, одержання привілеїв в адміністратора й т.п.

Сервер Kerberos KS можна розділити на дві частини: сервер автентифікації AS (Authentication Server) і сервер служби видачі мандатів TGS (Ticket Granting Service). Фізично дані сервери можуть бути сполучені. Інформаційними ресурсами, необхідними клієнтам З, управляє сервер інформаційних ресурсів RS. Передбачається, що сервери служби Kerberos надійно захищені від фізичного доступу зловмисників.

Мережні служби, що вимагають перевірки дійсності, і клієнти, які хочуть використати ці служби, реєструють в Kerberos свої секретні ключі. Kerberos зберігає базу даних про клієнтів й їхні секретні ключі. Наявність у цій базі даних секретних ключів кожного користувача й ресурсів мережі, що підтримують даний протокол, дозволяє створювати зашифровані повідомлення, що направляють клієнтові або серверу; успішне расшифрування цих повідомлень й є гарантією проходження автентифікації всіма учасниками протоколу.

Kerberos також створює *сеансові ключі* (session key), які видаються клієнтові й серверу (або двом клієнтам) і нікому більше. Сеансовий ключ використається для шифрування повідомлень, якими обмінюються дві сторони, і знищується після закінчення сеансу.

Область дії системи Kerberos поширюється на ту ділянку мережі, всі користувачі якого зареєстровані під своїми іменами й паролями в базі даних сервера Kerberos.

Як працює Kerberos

Загалом процес ідентифікації й автентифікації користувача в системі Kerberos версії 5 можна описати в такий спосіб (мал. 4.3).

Клієнт І3, бажаючи одержати доступ до ресурсу мережі, направляє запит серверу автентифікації AS. Сервер AS ідентифікує користувача за допомогою його імені й пароля й висилає клієнтові мандат на доступ до сервера служби виділення мандатів TGS (Ticket-Granting Service).

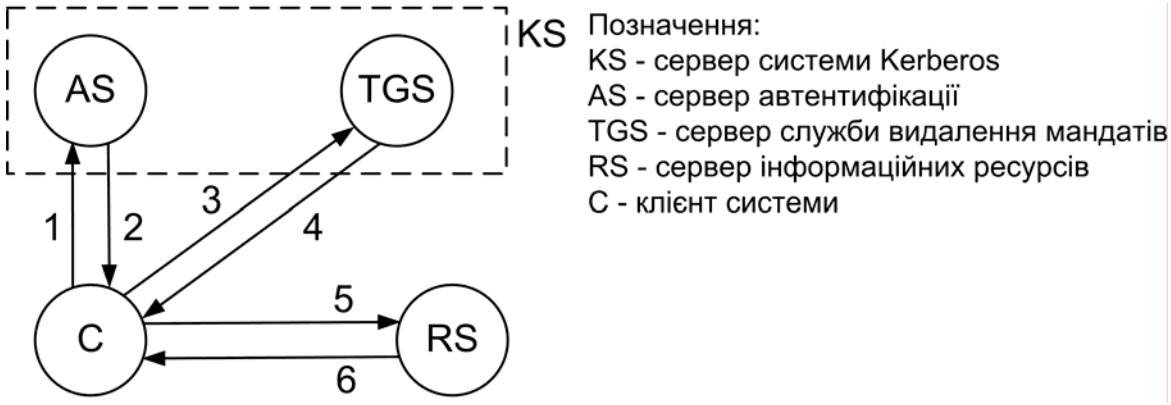

Рисунок 3.3 - Схема роботи протоколу Kerberos

Для використання конкретного цільового сервера інформаційних ресурсів *RS* клієнт *Із* запитує в TGS мандат на звертання до цільового сервера *RS*. Якщо все в порядку, TGS дозволяє використання необхідних ресурсів мережі й посилає відповідний мандат клієнтові С.

Основні кроки роботи системи Kerberos (рисунок 4.3):

1. $C \to AS$ - запит клієнта *C* к серверу *AS* на дозвіл звернутися до служби TGS.

2. $AS \to C$ - дозвіл (мандат) від сервера *AS* клієнтові *Зі* звернутися до служби TGS.

3. $C \to TGS$ - запит клієнта *C* к службі *TGS* на одержання допуску (мандата) до сервера ресурсів *RS*.

4. $TGS \to C$ - дозвіл (мандат) від служби *TGS* клієнтові *Із* для звертання до сервера ресурсів *RS*.

5. $C \to RS$ - запит інформаційного ресурсу (послуги) у сервера *RS*.

6. $RS \to C$ - підтвердження дійсності сервера *RS* і надання інформаційного ресурсу (послуги) клієнтові *C*.

Дана модель взаємодії клієнта із серверами може функціонувати тільки за умови забезпечення конфіденційності й цілісності переданої керуючої інформації. Без строгого забезпечення інформаційної безпеки клієнт Із не може відправляти серверам AS, TGS й RS свої запити й одержувати дозволи на доступ до обслуговування в мережі.

Щоб уникнути можливості перехоплення й несанкціонованого використання інформації, Kerberos застосовує при передачі будь-якої керуючої інформації в мережі систему багаторазового шифрування з використанням комплексу секретних ключів (секретний ключ клієнта, секретний ключ сервера, секретні сеансові ключі пари клієнт-сервер). Kerberos може використати різні симетричні алгоритми шифрування й хеш-функції, однак обов'язковими для підтримки встановлені алгоритми Triple DES й MD5.

У системі Kerberos використаються два типи вірчих документів: мандат (ticket) і автентифікатор (authenticator).

Мандат використається для безпечної передачі серверу ідентифікаційних даних клієнта, якому виданий цей мандат. У ньому також утримується інфор-

мація, що сервер може використати для перевірки того, що клієнт, що використає мандат, - це саме та особа, якій даний мандат був виданий.

Автентифікатор - це додатковий атрибут, пропонований разом з мандатом.

Надалі в цьому розділі буде застосовуватися система позначень, використовувана в документах Kerberos:

c - клієнт;

s - сервер;

a - мережна адреса клієнта;

v - початок і закінчення часу дії мандата;

t - мітка часу;

K_x - секретний ключ x;

$K_{x,в}$ - сеансовий ключ для x и в;

$\{m\}\ K_x$ - повідомлення т, шифроване секретним ключем K_x суб'єкта x;

$T_{x,в}$ - мандат x на використання в;

$Ax_{,в}$ - аутентифікатор x для в.

Мандат Kerberos

Мандат Kerberos має наступну форму:

$T_{c,s} = s, \{c, a, v, R_{c,s}\} K_s$.

Мандат надається одному клієнтові для доступу до строго певного сервера й на строго певний час. Він містить ім'я клієнта, його мережна адреса, початковий і кінцевий час дії клієнта й сеансовий ключ $K_{s,c}$, зашифровані на секретному ключі K_s сервера.

Якщо клієнт одержав мандат, він може використати його для доступу до сервера протягом проміжку часу, відведеного для даного мандата. Клієнт не може розшифрувати мандат (він не знає секретного ключа K_s сервера), але він може пред'явити його серверу в зашифрованій формі. Ніхто з, що підслухують у мережі не зможе прочитати або змінити мандат при передачі його по мережі.

Автентифікатор Kerberos

Автентифікатор Kerberos має наступну форму:

$A_{C,S} = s, \{c, a, v, K_{R,S}) K_S$.

Автентифікатор створюється клієнтом щораз, коли той хоче одержати доступ до цільового сервера. Автентифікатор містить ім'я клієнта, мітку часу й сеансовий ключ, зашифровані на сеансовому ключі $K_{C,S}$ загальному для клієнта й сервера.

На відміну від мандата, автентифікатор використається тільки один раз. Однак клієнт може генерувати автентифікатори в міру потреби (йому відомий загальний секретний ключ $K_{C,S}$). Використання автентифікатора переслідує дві мети. По-перше, автентифікатор містить деякий відкритий текст, зашифрова-

ний сеансовим ключем. Це доводить, що клієнтові відомий ключ. По-друге, зашифрований відкритий текст включає мітку часу. Ця мітка часу не дозволяє зловмисникові, що перехопив даний автентифікатор і мандат, використати їх через деякий час для успішного проходження процедури автентифікації.

Повідомлення Kerberos

В Kerberos версії 5 використається п'ять типів повідомлень (див. рисунок 3.3):

1. Клієнт-Kerberos: c,tgs.
2. Kerberos-клієнт: $\{K_{c,tgs}\}K_c\{T_{c,tgs}\}K_{tgs}$.
3. Клієнт-TGS: $\{A_{c,s}\}K_{c,tgs}\{T_{c,tgs}\}K_{tgs,s}$.
4. TGS-клієнт: $\{K_{c,s}\}K_{c,tgs}\{T_{c,s}\}K_s$.
5. Клієнт-сервер: $\{A_{c,s}\}K_{c,s}\{T_{c,s}\}K_s$.

Розглянемо використання цих повідомлень докладніше.

Одержання первісного мандата

У клієнта є частина інформації, що доводить його особистість, - його пароль. Зрозуміло, що не слід змушувати клієнта передавати пароль по мережі. Протокол Kerberos мінімізує ймовірність компрометації пароля, але при цьому не дозволяє користувачеві правильно ідентифікувати себе, якщо він не знає пароля.

Клієнт посилає на сервер автентифікації Kerberos повідомлення, що містить його ім'я й ім'я його сервера TGS (може бути кілька серверів TGS). На практиці користувач найчастіше просто вводить своє ім'я - і програма входу в систему надсилає запит.

Сервер автентифікації Kerberos шукає дані про клієнта у своїй базі даних. Якщо інформація про клієнта є в базі даних, Kerberos генерує сеансовий ключ $K_{c,tgs}$, що буде використатися для обміну даними між клієнтом й TGS. Kerberos шифрує цей сеансовий ключ секретним ключем клієнта K_c. Потім він створює для клієнта мандат на виділення мандата TGT (Ticket Granting Ticket), що доводить службі TGS дійсність клієнта. TGT зашифровується на секретному ключі TGS і містить ідентифікатори клієнта й сервера, сеансовий ключ пари TGS-клієнт, а також початковий і кінцевий час дії TGT. Сервер автентифікації посилає ці два зашифрованих повідомлення клієнтові.

Тепер клієнт приймає дані повідомлення, розшифровує перше повідомлення своїм секретним ключем K_c й одержує сеансовий ключ $K_{c,tgs}$. Секретний ключ є односпрямованою хеш-функцією клієнтського пароля, тому в законного користувача не буде ніяких проблем. Зловмисник не знає правильного пароля й, отже, не може розшифрувати відповідь сервера автентифікації. Тому зловмисник не може одержати мандат або сеансовий ключ.

Клієнт зберігає мандат TGT і сеансовий ключ, стираючи пароль і хеш-значення. Ця інформація знищується для зменшення ймовірності компрометації. Якщо зловмисник спробує скопіювати вміст пам'ять клієнта, він одержить тільки TGT і сеансовий ключ. Ці дані важливі, але тільки на час життя TGT Коли термін дії TGT мине, ці відомості стануть безглуздими. Тепер клієнт має можливість пройти автентифікацію в TGS-сервера за допомогою отриманого мандата TGT протягом усього терміну дії TGT, зазначеного в ньому.

Одержання серверних мандатів

Далі клієнт може одержати окремий мандат для кожної потрібної йому послуги. Із цією метою клієнт повинен надіслати запит у службу TGS (на практиці програмне забезпечення надсилає запит автоматично, тобто невидимо для користувача). Цей запит складається з мандата TGT й автентифікатора. Автентифікатор, зашифрований на ключі парного зв'язку клієнта й сервера TGS, містить ідентифікатори клієнта й сервера, що вимагається йому,, випадковий сеансовий ключ і мітку часу.

TGS, одержавши запит, розшифровує TGT своїм секретним ключем. Потім TGS використає включений в TGT сеансовий ключ, щоб розшифрувати автентифікатор. У завершення проводиться порівняння інформації, що втримується в автентифікаторі, з інформацією мандата. Точніше, мережна адреса клієнта у квитку звіряється з мережною адресою, зазначеною в запиті, а також рівняється мітка часу з поточним часом. Якщо все збігається, TGS дозволяє виконання запиту.

Перевірка міток часу припускає, що годинники всіх комп'ютерів синхронізовані, принаймні, з точністю до декількох хвилин. Якщо час, зазначений у запиті, значно відрізняється від сучасний момент, TGS уважає такий запит спробою повторення попереднього запиту.

Служба TGS повинна також відслідковувати правильність термінів дії автентифікаторів, тому що послуги сервера можуть запитуватися кілька разів послідовно з одним мандатом, але різними автентифікаторами. Інший запит з тим же мандатом і вже використаною міткою часу автентифікатора буде відкинутий.

У відповідь на вірний запит TGS надає клієнтові мандат для доступу до цільового сервера. TGS також створює сеансовий ключ для клієнта й цільового сервера, зашифрований сеансовим ключем, загальним для клієнта й TGS. Обоє ці повідомлення відправляються клієнтові. Клієнт розшифровує повідомлення й витягає сеансовий ключ.

Запит послуги

Тепер клієнт може довести свою дійсність цільовому серверу. Для успішного проходження автентифікації в цільового сервера клієнт створює автентифікатор, що складається з його імені, мережної адреси й мітки часу й зашифрований на сеансовому ключі “клієнт-сервер”, і відправляє його разом з манда-

том, зашифрованим на секретному ключі цільового сервера, що був переданий від служби TGS.

Прийнявши дані від клієнта, цільовий сервер проводить перевірку автентифікатора. Він розшифровує його за допомогою свого секретного ключа й витягає з нього сеансовий ключ “клієнт-сервер”. Мандат також піддається перевірці. Процедура перевірки схожа із процедурою, проведеної у випадку сесії “клієнт-TGS”, тобто перевіряється відповідність мережних адрес і тимчасової мітки. Якщо все в порядку, то сервер упевнений, що клієнт - саме той, за кого він себе видає,

Якщо додаток вимагає взаємної перевірки дійсності, сервер посилає клієнтові повідомлення, що складається з мітки часу, зашифрованої сеансовим ключем. Це доводить, що серверу відомі правильний секретний ключ і він може розшифрувати мандат і посвідчення. При необхідності клієнт і сервер можуть шифрувати подальші повідомлення загальним ключем. Тому що цей ключ відомий тільки їм, вони обоє можуть бути впевнені, що останнє повідомлення, зашифроване цим ключем, відправлено іншою стороною. На практиці вся ця складна процедура автентифікації виконується автоматично й не доставляє клієнтові яких-небудь значних незручностей.

Особливості міждоменної автентифікації

Kerberos може використатися й для міждоменної автентифікації. У випадку обігу клієнта в центр розподілу ключів KDC для доступу до сервера, що перебуває в іншому домені, KDC видає клієнтові *мандат переадресації* (refferal ticket) для звертання до KDC того домену, у якому перебуває необхідний сервер (рисунок 3.4).

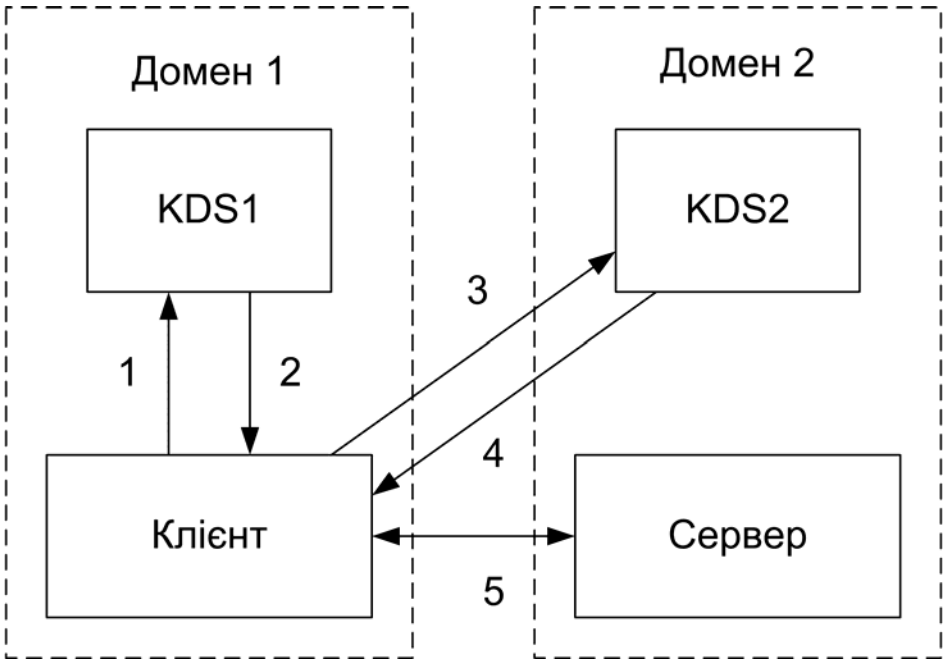

Рисунок 3.4 – Схема між доменної автентифікації в протоколі Kerberos

На малюнку прийняті наступні позначення

1. Запит на автентифікацію.
2. TGT для KDC.
3. Пред'явлення TGT для KDC.
4. Мандат доступу до сервера.
5. Автентифікація й обмін даними.

Мандат переадресації являє собою TGT, зашифрований на ключі парного зв'язку KDC двох доменов. У цьому випадку мандат на доступ до сервера надає клієнтові той KDC, у веденні якого перебуває запитуваний сервер.

Теоретично можливе використання Kerberos для автентифікації в мережах з безліччю доменів. Однак у цьому випадку (у зв'язку з кількістю обігів, що зростають пропорційно кількості доменів) прийде створити якийсь центральний домен, що здійснює однозначну переадресацію запитів конкретним KDC.

Безпека Kerberos

Хоча протокол Kerberos одержав широке поширення серед користувачів і піддавався численним доробкам, у результаті чого з'явилася його п'ята версія, у деяких випадках і він може стати об'єктом успішної атаки порушника.

Насамперед варто пам'ятати, що Kerberos, як і будь-який інший програмний засіб криптографічного захисту, працює в недовереному програмному середовищу. Недокументовані можливості або неправильна конфігурація даного середовища може привести до того, що відбудеться витік критичної інформації, наприклад вихід у середовище передачі сеансових ключів, що зберігаються на жорсткому диску, або даних відкритої інформації. Навіть у випадку зберігання ключів на час сеансу роботи користувача тільки в оперативній пам'яті збій в ОС може привести до того, що ключі будуть скопійовані на жорсткий диск.

При використанні на робочій станції із установленим ПЗ Kerberos багатокористувальницького режиму або при відсутності контролю доступу до робочої станції створюється потенційна можливість внесення закладень-програм-закладок або модифікації криптографічного ПЗ. Тому безпека Kerberos багато в чому залежить від надійності захисту робочої станції, на якій установлений даний протокол.

До самого протоколу Kerberos пред'являється ряд додаткових вимог, які докладно описані в RFC-1510. Приведемо тільки основні з них:

- служби Kerberos повинні бути захищені від атак, спрямованих на відмову в обслуговуванні;
- необхідна синхронізація системного часу всіх учасників системи, оскільки мітки часу беруть участь у процесі автентифікації;
- Kerberos не захищає від атак підбором пароля. Проблема в тім, що зберігається в KDC ключ користувача є результатом переробки його пароля за допомогою хэш-функции. У випадку слабкого пароля можливий його підбор;
- служби Kerberos повинні бути надійно захищені від всіх видів несанкціонованого доступу;

•отримані клієнтом мандати, а також секретні ключі повинні бути захищені від несанкціонованого доступу.

Невиконання зазначених вимог може стати причиною успішної атаки.

На сьогоднішній день протокол Kerberos є широко розповсюдженим засобом автентифікації. Kerberos може використатися в сполученні з різними криптографічними схемами, включаючи шифрування з відкритим ключем.

Протоколи, засновані на використанні односпрямованих ключових хеш-функций

Протоколи, представлені вище, можуть бути модифіковані шляхом заміни симетричного шифрування на шифрування за допомогою однобічної ключової хеш-функції. Це буває необхідно, якщо алгоритми блокового шифрування недоступні або не відповідають пропонованим вимогам (наприклад, у випадку експортних обмежень).

Своєрідність шифрування за допомогою однобічної хеш-функції полягає в тім, що воно, власне кажучи, є однобічним, тобто не супроводжується зворотним перетворенням - расшифровуванням на прийомній стороні. Обидві сторони (відправник й одержувач) використають ту саму процедуру однобічного шифрування.

Однобічна хеш-функція $h_K(.)$ із джерелом-ключем-параметром-ключем K, застосована до даних M, що шифруються, дає в результаті хеш-значення m (дайджест), що складається з фіксованого невеликого числа байтів (рисунок 3.5).

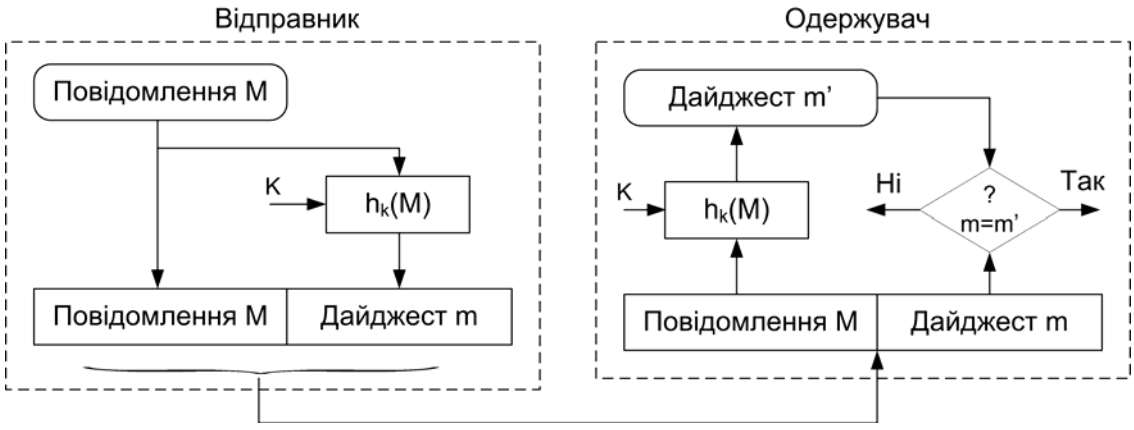

Рисунок 3.5 - Застосування для автентифікації однобічної хеш-функції із джерелом-ключем-параметром-ключем

Дайджест $m = h_K(M)$ передається одержувачеві разом з вихідним повідомленням M. Одержувач повідомлення, знаючи, яка однобічна хеш-функція була застосована для одержання дайджесту, заново обчислює її, використовуючи розшифроване повідомлення M. Якщо значення отриманого дайджесту m й обчисленого дайджесту m' збігаються, виходить, уміст повідомлення M не було піддано ніяким змінам.

Знання дайджесту не дає можливості відновити вихідне повідомлення, але дозволяє перевірити цілісність даних. Дайджест можна розглядати як свого роду контрольну суму для вихідного повідомлення. Однак між дайджестом і звичайною контрольною сумою є й істотне розходження. Контрольну суму використають як засіб перевірки цілісності переданих повідомлень по ненадійних лініях зв'язку. Це засіб перевірки не розраховано на боротьбу зі зловмисниками, яким у такій ситуації ніщо не заважає підмінити повідомлення, додавши до нього нове значення контрольної суми. Одержувач у такому випадку не помітить ніякої підміни.

На відміну від звичайної контрольної суми, при обчисленні дайджесту застосовуються секретні ключі. У випадку, якщо для одержання дайджесту використається однобічна хеш-функція із джерелом-ключем-параметром-ключем K, що відомий тільки відправникові й одержувачеві, будь-яка модифікація вихідного повідомлення буде негайно виявлена. На рисунку 4.6 показаний інший варіант використання однобічної хеш-функції для перевірки

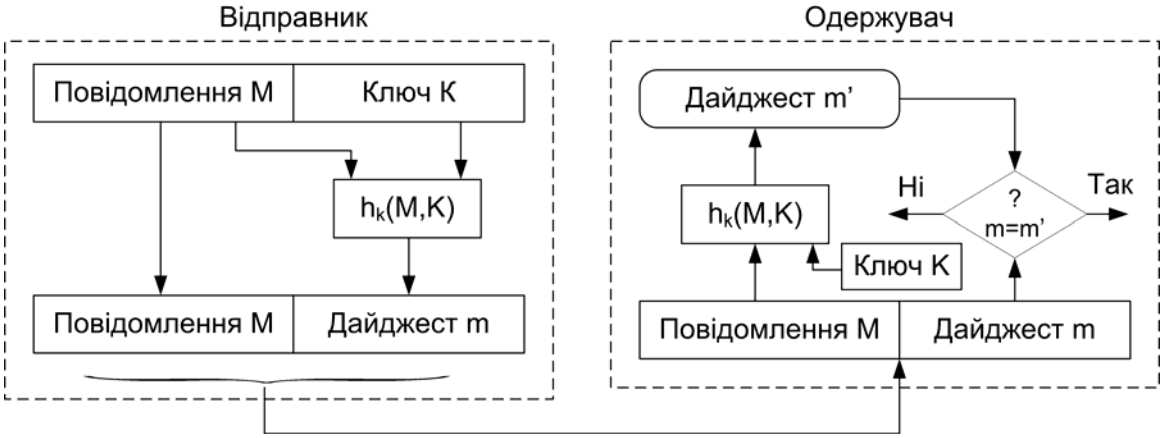

Рисунок 3.6 - Застосування однобічної хеш-функції до повідомлення, доповненому секретним ключем ДО

У цьому випадку однобічна хеш-функція $h(.)$ не має джерела-ключа-параметра-ключа, але зате застосовується не просто до повідомлення M, а до повідомлення, доповненому секретним ключем K, тобто відправник обчислює дайджест $m = h(M, K)$. Одержувач, витягаючи вихідне повідомлення M, також доповнює його тим же відомим йому секретним ключем K, після чого застосовує до отриманих даних однобічну хеш-функция $h(.)$. Результат обчислень - дайджест m' рівняється з отриманим по мережі дайджестом m.

При використанні для автентифікації однобічних функцій шифрування в розглянуті вище протоколи необхідно внести наступні зміни:

- функція симетричного шифрування E_k заміняється функцією h_k;
- що перевіряє замість установлення факту збігу значень у полях у розшифрованих повідомленнях з передбачуваними значеннями обчислює значення односпрямованої функції й порівнює його з отриманим від іншого учасника обміну інформацією;

• для забезпечення можливості незалежного обчислення значення односпрямованої функції одержувачем повідомлення в протоколі 1 мітка часу t_A повинна передаватися додатково у відкритому виді, а в повідомленні (2) протоколу 3 випадкове число r_A повинне передаватися додатково у відкритому виді.

Модифікований варіант протоколу 3 з урахуванням сформульованих змін має наступну структуру:

$$A \leftarrow B : r_B \quad (1)$$

$$A \rightarrow B : r_A, h_K(r_A, r_B, B) \quad (2)$$

$$A \leftarrow B : h_K(r_A, r_B, A) \quad (3)$$

Помітимо, що в третє повідомлення протоколу включене поле А. Результуючий протокол забезпечує взаємну автентифікацію й відомий як протокол SKID 3.

3.3.3 Строга автентифікація, заснована на асиметричних алгоритмах

У протоколах строгої автентифікації можуть бути використані асиметричні алгоритми з відкритими ключами. У цьому випадку що доводить може продемонструвати знання секретного ключа одним з наступних способів:

• розшифрувати запит, зашифрований на відкритому ключі;

• поставити свій цифровий підпис на запиті.

Пари ключів, необхідна для автентифікації, не повинна використатися для інших цілей (наприклад, для шифрування) по міркуваннях безпеки. Варто також застерегти потенційних користувачів про те, що обрана система з відкритим ключем повинна бути стійкої до атак з вибіркою шифрованого тексту навіть у тому випадку, якщо порушник намагається одержати критичну інформацію, видавши себе за що перевіряє й діючи від його імені.

Автентифікація з використанням асиметричних алгоритмів шифрування

Як приклад протоколу, побудованого на використанні асиметричного алгоритму шифрування, можна привести наступний протокол автентифікації:

$$A \leftarrow B : h(r), B, P_A(r, B) \quad (1)$$

$$A \rightarrow B : r \quad (2)$$

Учасник B вибирає випадковим образом r й обчислює значення $x = h(r)$ (значення x демонструє знання r без розкриття самого значення r), далі він обчислює значення $e = P_A(r, B)$. Під P_A мається на увазі алгоритм асиметричного шифрування (наприклад, RSA), а під $h(.)$ - хэш-функция. Учасник B відправляє повідомлення (1) учасникові A. Учасник A розшифровує $e = P_A(r, B)$ й одержує значення r^1 й B^1, а також обчислює $x^1 = h(r^1)$. Після цього проводиться ряд порівнянь, що доводять, що $x = x^1$ й що отриманий ідентифікатор B^1 дійсно вказує на учасника B. У випадку успішного проведення порівняння

учасник A посилає r. Одержавши його, учасник B перевіряє, чи то це значення, що він відправив у першому повідомленні.

Як наступний приклад приведемо модифікований протокол Нидхэма й Шредера, заснований на асиметричному шифруванні. Досить докладно даний протокол описується в розділі, присвяченому розподілу ключової інформації, оскільки основний варіант протоколу використається для автентифікаціонного обміну ключової інформації.

Розглядаючи варіант протоколу Нідхема й Шредера, використовуваний тільки для автентифікації, будемо мати на увазі під P_B алгоритм шифрування відкритим ключем учасника B. Протокол має наступну структуру:

$$A \to B : P_B(r_1, A) \quad (1)$$

$$A \leftarrow B : P_A(r_2, r_1) \quad (2)$$

$$A \leftarrow B : r_2 \quad (3)$$

Автентифікація, заснована на використанні цифрового підпису

У рекомендаціях стандарту X.509 специфікована схема автентифікації, заснована на використанні цифрового підпису, міток часу й випадкових чисел. Для опису даної схеми автентифікації введемо наступні позначення:

- t, r й $r_в$ - тимчасова мітка й випадкові числа відповідно;
- S_A - підпис, згенерований учасником A;
- S_B - підпис, згенерований учасником B;
- *cert* - сертифікат відкритого ключа учасника A;
- *cert* - сертифікат відкритого ключа учасника B.

Якщо учасники мають автентичні відкриті ключі, отримані друг від друга, тоді можна не користуватися сертифікатами, у противному випадку вони служать для підтвердження дійсності відкритих ключів.

Як приклади приведемо наступні протоколи автентифікації:

1. Однобічна автентифікація із застосуванням міток часу:

$$A \to B : cert_A, t_A, B, S_A(t_A, B) \quad (1)$$

Після прийняття даного повідомлення учасник B перевіряє правильність мітки часу t_A, отриманий ідентифікатор B й, використовуючи відкритий ключ із сертифіката $sertA$, коректність цифрового підпису $S_A(t_A, B)$.

2. Однобічна автентифікація з використанням випадкових чисел:

$$A \leftarrow B : r_B \quad (1)$$

$$A \to B : cert_A, r_A, B, S_A(r_A, r_B, B \quad (2)$$

Учасник B, одержавши повідомлення від учасника A, переконується, що саме він є адресатом повідомлення; використовуючи відкритий ключ учасника A, узятий із сертифіката $sertA$, перевіряє коректність підпису $S_A(r_A, r_B, B)$ під числом r_A, отриманим у відкритому виді, числом r_B, що було відіслано в першому повідомленні, і його ідентифікатором B. Підписане випадкове число r_A використається для запобігання атак з вибіркою відкритого тексту.

3. Двостороння автентифікація з використанням випадкових чисел:

$$A \leftarrow B : r_B \quad (1)$$

$$A \rightarrow B : cert_A, r_A, B, S_A(r_A, r_B, B) \quad (2)$$

$$A \leftarrow B : cert_B, A, S_B(r_A, r_B, A) \quad (3)$$

У даному протоколі обробка повідомлень (1) і (2) виконується так само, як й у попередньому протоколі, а повідомлення (3) обробляється аналогічно повідомленню (2).

3.4 Біометрична автентифікація користувача

Процедури ідентифікації й автентифікації користувача можуть базуватися не тільки на секретній інформації, який володіє користувач (пароль, персональний ідентифікатор, секретний ключ і т.п.). Звичні системи автентифікації не завжди задовольняють сучасним вимогам в області інформаційної безпеки, особливо якщо мова йде про відповідальні додатки (онлайнових фінансових додатках, доступі до вилучених баз даних і т.п.).

Останнім часом все більше поширення одержує біометрична автентифікація користувача, що дозволяє впевнено автентифікувати потенційного користувача шляхом виміру фізіологічних параметрів і характеристик людини, особливостей його поводження. Використання рішень, заснованих на біометричній технології, дозволяє в ряді випадків поліпшити положення справ в області автентифікації.

Для методів автентифікації, заснованих на використанні багаторазових паролів, характерний наступний недолік: багаторазовий пароль може бути скомпрометований безліччю способів. Недоліком методів, пов'язаних з використанням токенів, є можливість втрати, крадіжки, дублювання токенов - носіїв критичної інформації. Біометричні методи, що використають для ідентифікації унікальні характеристики користувача, вільні від перерахованих недоліків.

Відзначимо основні достоїнства біометричних методів автентифікації користувача в порівнянні із традиційними:

- високий ступінь вірогідності автентифікації по біометричних ознаках через їхню унікальність;
- невіддільність біометричних ознак від дієздатної особистості;
- труднощі фальсифікації біометричних ознак.

Як біометричні ознаки, які активно використаються при автентифікації потенційного користувача, можна виділити наступні:

- відбитки пальців;
- геометричну форму кисті руки;
- форму й розміри особи;
- особливості голосу;
- візерунок райдужної оболонки й сітківки ока.

Розглянемо типову схему функціонування біометричної підсистеми автентифікації. При реєстрації в системі від користувача потрібно продемонструвати один або кілька разів свої характерні біометричні ознаки. Ці ознаки (відомі

як справжні) реєструються системою як контрольний образ (біометричний підпис) законного користувача. Цей образ користувача зберігається системою в електронній формі й використається для перевірки ідентичності кожного, хто видає себе за законного користувача. Залежно від збігу або розбіжності сукупності пред'явлених ознак із зареєстрованими в контрольному образі їх що пред'явив зізнається законним користувачем (при збігу) чи ні (при розбіжності). З погляду споживача, ефективність біометричної автентифікаційної системи характеризується двома параметрами:

- коефіцієнтом помилкових відмов FRR (false-reject rate);
- коефіцієнтом помилкових підтверджень FAR (false-alarm rate).

Помилкова відмова виникає тоді, коли система не підтверджує особистість законного користувача (типові значення FRR становлять порядку однієї помилки на 100). *Помилкове підтвердження* відбувається у випадку підтвердження особистості незаконного користувача (типові значення FAR становлять порядку однієї помилки на 10000). Коефіцієнт помилкових відмов і коефіцієнт помилкових підтверджень зв'язані один з одним: кожному коефіцієнту помилкових відмов відповідає певний коефіцієнт помилкових підтверджень.

У зробленій біометричній системі обидва параметри помилки повинні бути дорівнюють нулю. На жаль, біометричні системи не ідеальні, тому доводиться чимсь жертвувати. Звичайно системні параметри набудовують так, щоб домогтися необхідного коефіцієнта помилкових підтверджень, що визначає відповідний коефіцієнт помилкових відмов.

До теперішнього часу розроблені й продовжують удосконалюватися технології автентифікації по відбитках пальців, райдужній оболонці ока, за формою кисті руки й долоні, за формою й розміром особи, по голосі й “клавіатурному почерку”.

Найбільше число біометричних систем як параметр ідентифікації використають відбитки пальців (дактилоскопічні системи автентифікації). Такі системи прості й зручні, мають високу надійність автентифікації.

Дактилоскопічні системи автентифікації

Однієї з основних причин широкого поширення таких систем є наявність більших банків даних по відбитках пальців. Основними користувачами подібних систем в усім світі є поліція, різні державні й деякі банківські організації.

У загальному випадку біометрична технологія розпізнавання відбитків пальців заміняє захист доступу з використанням пароля. Більшість систем використають відбиток одного пальця, що користувач надає системі.

Основними елементами дактилоскопічної системи автентифікації є:

- сканер;
- ПЗ ідентифікації, що формує ідентифікатор користувача;
- ПЗ автентифікації, що проводить порівняння відсканованого відбитка пальця з наявними в базі даних “паспортами” користувачів.

Дактилоскопічна система автентифікації працює в такий спосіб. Спочатку виконується реєстрація користувача. Як правило, проводиться кілька варіантів сканування в різних положеннях пальця на сканері. Зрозуміло, що зразки будуть небагато відрізнятися й потрібно сформувати деякий узагальнений зразок, "паспорт". Результати запам'ятовуються в базі даних автентифікації. При автентифікації проводиться порівняння відсканованого відбитка пальця з "паспортами", що зберігаються в базі даних.

Завдання формування "паспорта", так само як і завдання розпізнавання пропонованого зразка, спрямована на розпізнавання образів. Для цього використаються різні алгоритми, що є ноу-хау фірм-виробників подібних пристроїв.

Сканери відбитків пальців

Багато виробників всі частіше переходять від дактилоскопічного встаткування на базі оптики до продуктів, заснованим на інтегральних схемах.

У традиційних пристроях сканування відбитків пальців основним елементом є маленька оптична камера для запису характерного малюнка пальця. Ряд виробників усе ще використають цю технологію. Однак усе більше виробників дактилоскопічного встаткування проявляють увагу до сенсорних пристроїв на базі інтегральних схем. Така тенденція відкриває нові сфери застосування автентифікації на основі відбитків пальців.

Компанії, що розробляють подібні технології, використають різні засоби одержання відбитків пальців, у тому числі реалізуючі електричні, електромагнітні й інші методи.

Один з нових сканерів вимірює ємнісний опір ділянок шкіри для формування зображення відбитка пальця. Наприклад, сенсорний дактилоскопічний пристрій компанії Veridicom збирає інформацію, зчитуючи ємнісний опір за допомогою твердотільного напівпровідникового датчика.

Принцип дії сенсора такий: палець, прикладений до цього приладу, виконує роль однієї із пластин конденсатора (рисунок 3.7). Інша пластина, розташована на поверхні сенсора, являє собою кремнієву мікросхему з 90000 чутливими пластинками конденсатора. Опуклості подушечки пальця стосуються поверхні датчика. Чутливі ємнісні датчики вимірюють зміну сили електричного поля між опуклостями й улоговинками подушечки пальця, що дозволяє визначити відстані до опуклостей й улоговинок й одержати зображення відбитка пальця.

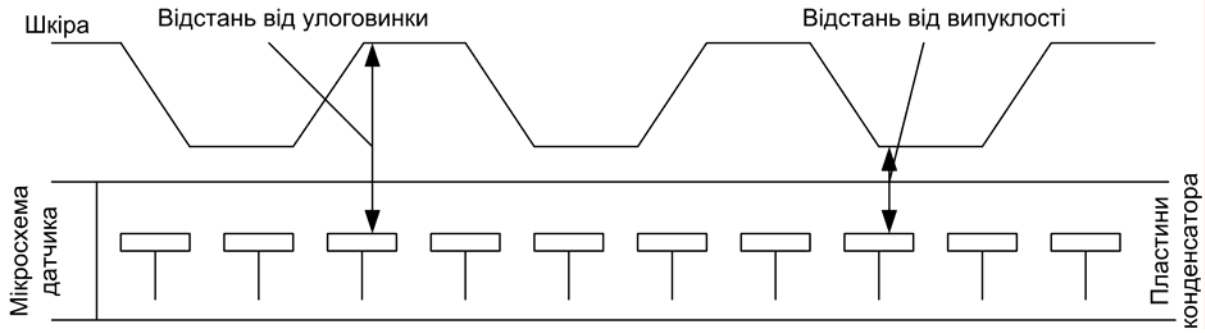

Рисунок 3.7 - Ємнісна чутливість - один зі способів, за допомогою якого напівпровідникові сенсори розрізняють відбитки пальців

Отримана інформація перетвориться у відеосигнал і потім обробляється відповідно до алгоритму, що формує зразок зображення. Саме за цим зразком здійснюється верифікація користувача.

Інший метод, використовуваний компанією AuthenTec, робить сенсорну перевірку на основі інтегральних схем ще більш точної. Дактилоскопічний зчитувач містить прямокутну поверхню для перевірки відбитків пальців, називану *сенсорною матрицею*. Це не що інше як активний масив мініатюрних антен, що складає більш ніж з 16000 елементів із прозорим покриттям, що захищає від подряпин й інших зовнішніх впливів. Сенсорна матриця оточена напрямним кільцем, що передає слабкі сигнали, що вловлюють окремими елементами-антенами.

Сканування більше глибокого шару шкіри (під эпидермисом), де перебувають унікальні опуклості й западини, що створюють малюнок шкіри пальця, виконується в такий спосіб. Коли користувач доторкається до поверхні мікросхеми, що направляє кільце асоціює слабкий сигнал з підшкірним шаром пальця. Даний сигнал створює цифровий зразок, що відбиває унікальну підшкірну структуру - у цьому полягає відмітна перевага технології AuthenTec. Використовуючи підсилювачі високого дозволу (менш 1 пикселя) і інші засоби відновлення сигналу, ПО TruePrint управляє вихідними сигналами з тисяч окремих сенсорних елементів і формує на їхній основі точне, неспотворене подання відбитка пальця, після чого переводить його в зразок, використовуваний згодом для верифікації.

Сенсорний пристрій AuthenPad компанії AuthenTec являє собою квадрат зі стороною 20 мм товщиною 1,4 мм.

Продукти на базі інтегральних схем мають значно менші розміри, чим оптичні зчитувачі, і тому їх простіше реалізувати в широкому спектрі периферійних пристроїв.

Ряд виробників комбінують біометричні системи зі смарт-картками й картками-ключами. Наприклад, у біометричній ідентифікаційній смарт-картці Authentic реалізований наступний підхід. Зразок відбитка пальця користувача зберігається в пам'яті картки в процесі внесення в списки ідентифікаторів користувачів, установлюючи відповідність між зразком й особистим ключем шифрування. Потім, коли користувач уводить смарт-картку в зчитувач і прикладає палець до сенсора, ключ засвідчує його особистість. Комбінація біометричних пристроїв і смарт-картка є вдалим рішенням, що підвищує надійність процесів автентифікації й авторизації.

Невеликий розмір і невисока ціна датчиків відбитків пальців на базі інтегральних схем перетворює їх в ідеальний інтерфейс для систем захисту. Їх можна буде вбудовувати в брелок для ключів, і користувачі одержать універсальний ключ, що забезпечить захищений доступ до всьому, починаючи від комп'ютерів до вхідних дверей, дверцят автомобілів і банкоматів.

Системи автентифікації за формою долоні

Подібні системи використають сканери форми долоні, звичайно встановлювані на стінах. Слід зазначити, що переважна більшість користувачів предпочитают системи цього типу.

Пристрою зчитування форми долоні створюють об'ємне зображення долоні, вимірюючи довжину пальців, товщину й площу поверхні долоні. Наприклад, продукти компанії Recognition Systems виконують більше 90 вимірів, які перетворяться в 9-розрядний зразок для подальших порівнянь. Цей зразок може бути збережений локально на індивідуальному сканері долоні або в централізованій базі даних.

За рівнем доходів пристрою сканування форми долоні посідають друге місце серед біометричних пристроїв, однак рідко застосовуються в мережному середовищі через високу вартість і великий розмір. Однак сканери форми долоні добре підходять для обчислювальних середовищ зі строгим режимом безпеки й напруженим трафиком, включаючи серверні кімнати. Вони досить точні й мають досить низький коефіцієнт помилкової відмови FRR (False Rejection Rate), тобто відсотком відхилених законних користувачів.

Системи автентифікації по особі й голосу

Ці системи є найбільш доступними через їхню дешевину, оскільки більшість сучасних комп'ютерів мають відео- і аудиосредства. Системи даного класу застосовуються при вилученій ідентифікації суб'єкта доступу в телекомунікаційних мережах.

Технологія сканування рис особи підходить для тих додатків, де інші біометричні технології непридатні. У цьому випадку для ідентифікації й верифікації особистості використаються особливості очей, носа й губ. Виробники пристроїв розпізнавання чорт особи використають власні математичні алгоритми для ідентифікації користувачів

Дослідження, проведені компанією International Biometric Group, говорять про те, що співробітники багатьох організацій не довіряють пристроям розпізнавання по рисах особи почасти через те, що камера їх фотографує, а потім виводить знімки на екран монітора; при цьому багато хто побоюються, що використовувана камера - низької якості. Крім того, за даними цієї компанії, сканування рис особи - єдиний метод біометричної автентифікації, що не вимагає згоди на виконання перевірки (і може здійснюватися схованою камерою), а тому має негативний для користувачів підтекст.

Слід зазначити, що технології розпізнавання чорт особи вимагають подальшого вдосконалювання. Більшість алгоритмів розпізнавання чорт особи чутливі до коливань у висвітленні, викликаним зміною інтенсивності сонячного світла протягом дня. Зміна положення особи також може вплинути на пізнаванність. Розходження в положенні в 15° між запитуваним зображенням і зображенням, що перебуває в базі даних, *прямо* позначається на ефективності. При розходженні в 45° розпізнавання стає неефективним.

Системи автентифікацій за голосом економічно вигідні по тим же причинам, що й системи розпізнавання за рисами особи. Зокрема, їх можна встановлювати з устаткуванням (наприклад, мікрофонами), що поставляють у стандартній комплектації з багатьма ПК.

Системи автентифікації по голосі при записі зразка й у процесі наступної ідентифікації опираються на такі унікальні для кожної людини особливості голосу, як висота, модуляція й частота звуку. Ці показники визначаються фізичними характеристиками голосового тракту й унікальні для кожної людини. Розпізнавання голосу вже застосовується замість набору номера в певних системах Sprint. Такий вид розпізнавання голосу відрізняється від розпізнавання мови. У той час як технологія розпізнавання мови інтерпретує те, що говорить абонент, технологія розпізнавання голосу абонента підтверджує особистість мовця.

Оскільки голос можна просто записати на плівку або інші носії, деякі виробники вбудовують у свої продукти операцію запиту-відповіді. Ця функція пропонує користувачеві при вході відповісти на попередньо підготовлений і регулярно мінливий запит: наприклад, такий: “Повторіть числа 0, 1, 3”.

Устаткування автентифікації по голосі більше придатне для інтеграції в додатки телефонії, чим для входу в мережу. Звичайно воно дозволяє абонентам одержати доступ у фінансові або інші системи за допомогою телефонного зв'язку.

Технології розпізнавання мовця мають деякі обмеження. Різні люди можуть говорити схожими голосами, а голос будь-якої людини може мінятися згодом залежно від самопочуття, емоційного стану й віку. Більше того, різниця в модифікації телефонних апаратів й якість телефонних з'єднань можуть серйозно ускладнити розпізнавання.

Оскільки голос сам по собі не забезпечує достатньої точності, розпізнавання по голосі варто сполучати з іншими биометриками, такими як розпізнавання рис особи або відбитків пальців.

Системи автентифікації по візерунку райдужної оболонки й сітківки ока

Ці системи можуть бути розділені на два класи:

- що використовують малюнок райдужної оболонки ока;
- що використовують малюнок кровоносних посудин сітківки ока.

Сітківка людського ока являє собою унікальний об'єкт для автентифікації. Малюнок кровоносних посудин очного дна відрізняється навіть у близнюків. Оскільки ймовірність повторення параметрів райдужної оболонки й сітківки ока має порядок 10^{-78}, такі системи є найбільш надійними серед всіх біометричних систем. Такі засоби ідентифікації застосовуються там, де потрібен високий рівень безпеки (наприклад, у режимних зонах військових й оборонних об'єктів).

Згідно даним консалтингової компанії International Biometric Group з Нью-Йорка, за рівнем попиту найбільш популярною технологією стало скану-

вання відбитків пальців. За рівнем продажів біометричних пристроїв 44% доводиться на дактилоскопічні сканери. Системи розпізнавання чорт особи посідають друге місце за рівнем попиту, що становить 14%, далі випливають пристрою розпізнавання за формою долоні (13%), по голосі (10%) і райдужній оболонці ока (8%). Пристрою верифікації підпису в цьому списку становлять 2%. За прогнозами дослідницького центра ПОЗНАЧКА Group, рівень продажів цих пристроїв в усім світі в 2003 році повинен досягти 900 мільйонів доларів.

Біометричний підхід дозволяє спростити процес з'ясування “хто є хто”. При використанні дактилоскопічних сканерів і пристроїв розпізнавання голосу для входу в мережі співробітники позбуваються від необхідності запам'ятовувати складні паролі. Ряд компаній інтегрують біометричні можливості в системи однократної автентифікації SSO (Single Sign-On) масштабу підприємства. Подібна консолідація дозволяє мережним адміністраторам замінити служби однократної автентифікації паролів біометричними технологіями.

Однієї з перших областей широкого застосування біометричної автентифікації особистості стануть *мобільні системи.* Проблема не зводиться тільки до втрат комп'ютерів через крадіжки; порушення захисту інформації може привести до значно більшого збитку. Крім того, ноутбуки часто надають доступ до корпоративної мережі через програмні з'єднання (виконувані за допомогою паролів, що зберігаються на мобільних комп'ютерах).

Твердотільні датчики відбитків пальців - невеликі, недорогі й низько енергоємні - дозволяють вирішити ці проблеми. За допомогою відповідного програмного забезпечення ці пристрої дають можливість виконувати автентифікацію для чотирьох рівнів доступу до інформації, що зберігається на мобільному комп'ютері: реєстрації, виходу з режиму збереження екрана, завантаження й дешифрування файлів.

Біометрична автентифікація користувача може відігравати серйозну роль у шифруванні у вигляді модулів блокування доступу до секретного ключа, що дозволяє скористатися цією інформацією тільки щирому власникові приватного ключа. Власник може потім застосовувати свій секретний ключ для шифрування інформації, переданої по приватних мережах або по Internet.

Ахіллесовою п'ятою багатьох систем шифрування є проблема безпечного зберігання самого криптографічного секретного ключа. Найчастіше доступ до ключа довжиною 128 або навіть більше розрядів захищений лише паролем з 6 символів, тобто 48 розрядів. Відбитки пальців забезпечують набагато більше високий рівень захисту й, на відміну від пароля, їх неможливо забути.

4. РЕАЛІЗАЦІЯ ПОЛІТИКИ БЕЗПЕКИ В СУЧАСНИХ СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

4.1 Типові методи та засоби реалізації політики безпеки системи електронного документообігу

Для захисту СЕД використаються традиційні засоби:

- ідентифікація, автентифікація й авторизація об'єктів і суб'єктів (так, до питань авторизації в СЕД ставляться механізми розмежування доступу до даних і функцій системи — це, наприклад, наявність можливості в керівника відділу переглядати всі документи, над якими працюють співробітники відділу, у той час як кожен співробітник бачить лише свою частину роботи й не бачить документи, над якими працюють інші; кожний з документів може мати встановлені для нього права доступу на читання, зміну, видалення; корисно виділяти групи користувачів і делегувати права їхнього доступу до документів);
- керування доступом (дозволяє визначати для кожного документа й для кожної ПП правочинних користувачів й їхнього права);
- мережне екранування;
- засоби контролю імпортованих програм;
- криптографія;
- електронний цифровий підпис.

Розглянемо ці засоби стосовно до захисту від різних загроз.

Захист ЕДО від загроз конфіденційності здійснюється за допомогою стеганографії й криптографії. Стеганографія займається проблемою приховання від зловмисника самого факту передачі повідомлення. Найчастіше це досягається за рахунок введення в повідомлення додаткових бітів, що не псує якості зображення. Виявити заховане в такий спосіб повідомлення малого обсягу у великому обсязі інформації, не знаючи методу приховання й не маючи “чистого” варіанта файлу, досить складно. Загальний недолік стеганографічних методів захисту інформації — проблема збереження в таємниці самого методу приховання.

Криптографія має на меті приховання тексту повідомлення, роблячи його не читають для небажаних очей. При цьому допускається, що зловмисник знає не тільки сам факт передачі повідомлення, але й саме повідомлення, можливо, його приблизний або навіть точний текст. Допускається знання супротивником методу шифрування. У таємниці від зловмисника повинен залишатися тільки секретний параметр шифрування — ключ.

Для СЕД найчастіше застосовується два підходи.

3. Абонентське шифрування конфіденційної інформації — шифрування переданих між абонентами ІТС електронних документів. Використається схема абонентського шифрування із закритим розподілом ключів шифрування між абонентами, на базі повної матриці ключів (кожній парі абонентів системи відповідає свій секретний ключ для передачі шифрованих документів між ними). Достоїнство цього методу в тім, що алгоритм шифрування забезпечує доступ до переданої інформації тільки тим особам, яким дана інформація призначена.

4. Комплексний захист конфіденційності переданих між абонентами ІТС

електронних документів з одночасним стиском (архівуванням) документів, забезпеченням їхньої цілісності й автентифікація автора за допомогою ЕЦП. Обробка документів виробляється безпосередньо перед передачею або після прийому їхніми звичайними засобами електронної пошти.

Захист цілісності ЕДО ділиться на підзавдання захисту від несанкціонованої зміни, підробки й пропажі. Рішення перших двох проблем здійснюється застосуванням ЕЦП, заснованої на криптографії з відкритим ключем. Рішення проблеми пропажі документа лежить поза криптографією — тут потрібне створення резервних копій з носіїв інформації, їхнє дублювання й строгий облік документів. При передачі документа по каналах зв'язку потрібні захищені протоколи передачі даних (типу SSL, TLS або інших), що надають можливості одержання підтвердження про доставку, що здійснюють передачу даних різними маршрутами, і т.ін.

Захист ЕДО від загроз доступності, або від атак типу “відмова в обслуговуванні”, реалізується на рівні операційної системи, програмного й апаратного забезпечення установкою відповідних “латок”. Загроза полягає у відмові легальному (санкціонованому) користувачеві одержати доступ до інформації з боку системи. Способів створити ситуацію відмови в обслуговуванні, як буде описано далі, багато, починаючи від примітивних багаторазових спроб входу в систему від імені користувача до блокування його облікового запису й закінчуючи застосуванням хакерських атак на сервер типу “затоплення” повторюваними пакетами.

Підкреслимо, що захист СЕД досягається не окремими рішеннями, а системою добре продуманих мер, включаючи комплекс адміністративних процедур. Можливі створення системи захисту СЕД як єдиного цілого або розробка підсистем безпеки для окремих інформаційних комплексів СЕД. Незалежно від цього СЕД повинні мати рішення по забезпеченню ІБ у таких важливих областях застосування, як, наприклад, планування відновлення після НСД, розподілене зберігання даних, керування пристроями й сховищами даних, резервне копіювання й архівування й багато чого іншого.

4.2 Реалізація політики безпеки в СЕД DIRECTUM

Система електронного документообігу DIRECTUM [10] забезпечує високу надійність зберігання документів і швидкий доступ до них, при цьому в DIRECTUM представлені різні механізми забезпечення безпеки роботи з електронними документами.

4.2.1 Забезпечення схоронності документів

У більшості випадків електронні документи, створювані співробітниками, розташовуються на локальних жорстких дисках їхніх комп'ютерів. Крім того, що це незручно, неефективно з погляду взаємодії співробітників організації, не забезпечує розмежування прав доступу до документів, це також приводить до втрат документів, неможливості їх централізованого резервного копіювання.

Документи в системі DIRECTUM розташовуються в базі даних SQL-сервера, що забезпечує їхнє безпечне зберігання: документ не може бути загублений або знищений, тому що середовище зберігання документів повністю контролюється системою DIRECTUM, забезпечується регулярне резервне копіювання бази даних, доступ до даних обмежений тільки клієнтським додатком DIRECTUM.

Обмеження доступу до даних системи тільки за допомогою клієнтського додатка й API (об'єктної моделі) системи є одним з найважливіших вимог до системи електронного документообігу. Якщо в користувача з'являється можливість виконати прямий SQL-запит і спустошити таблиці бази даних (наприклад, “truncate table ...”), або видалити файл із файл-серверного сховища, це говорить про низьку безпеку системи.

4.2.2 Забезпечення безпечного доступу до електронних документів

Будь-який користувач у системі DIRECTUM працює під своїм ім'ям і паролем. При цьому підтримується можливість використання імені й пароля, з яким користувач увійшов в Windows (так звана Windows-автентифікація). Це дозволяє вирішити ряд проблем безпечного доступу в системі електронного документообігу. У першу чергу, це надійність обираних користувачами паролів. Не секрет, що користувачі схильні призначати прості для запам'ятовування (а виходить, і для підбора) паролі; за рахунок же застосування політик безпеки домену Windows паролі облікових записів домену будуть стійкими до злому. Другою істотною перевагою Windows-автентифікації є можливість інтеграції з апаратними засобами авторизації (смарт-карти, біометричні пристрої), що дозволяє забезпечити максимальний захист комп'ютера від його використання при відсутності користувача-власника сеансу.

Зі зберіганням документів у єдиній базі даних стає можливим повноцінне розмежування доступу до документів. В DIRECTUM можливе завдання прав доступу на кожен документ. Існує чотири типи прав: права відсутні, є права на перегляд, права на зміну й повні права на документ.

Права можуть задаватися як для окремих користувачів, так і для груп користувачів. Права перевіряються не тільки при роботі з візуальною частиною системи, але при доступі через об'єктну модель системи із зовнішніх додатків.

Розширює можливості обмеження доступу користувачів до документів системи DIRECTUM шифрування документів. Щоб сховати тексти документів від очей осіб, яким доступ до картки документа забороняти не можна (у т.ч. й адміністраторів системи), використається шифрування текстів документів.

Доступні два типи шифрування: шифрування на основі паролів і шифрування на основі сертифікатів; можливо їхнє комбіноване використання.

Шифрування на основі паролів забезпечує початковий рівень захисту тексту документів. Користувач указує для документа, що він буде шифруватися на основі пароля, указує пароль, і при збереженні змін тіло документа шифрується. При відкритті документа будь-яким користувачем, що має право на перегляд, запитується пароль. Передача пароля потрібним особам, забезпечення йо-

го конфіденційності й схоронності повністю залежить від власника документа (користувача, що має повні права). При втраті пароля текст документа відновленню не підлягає.

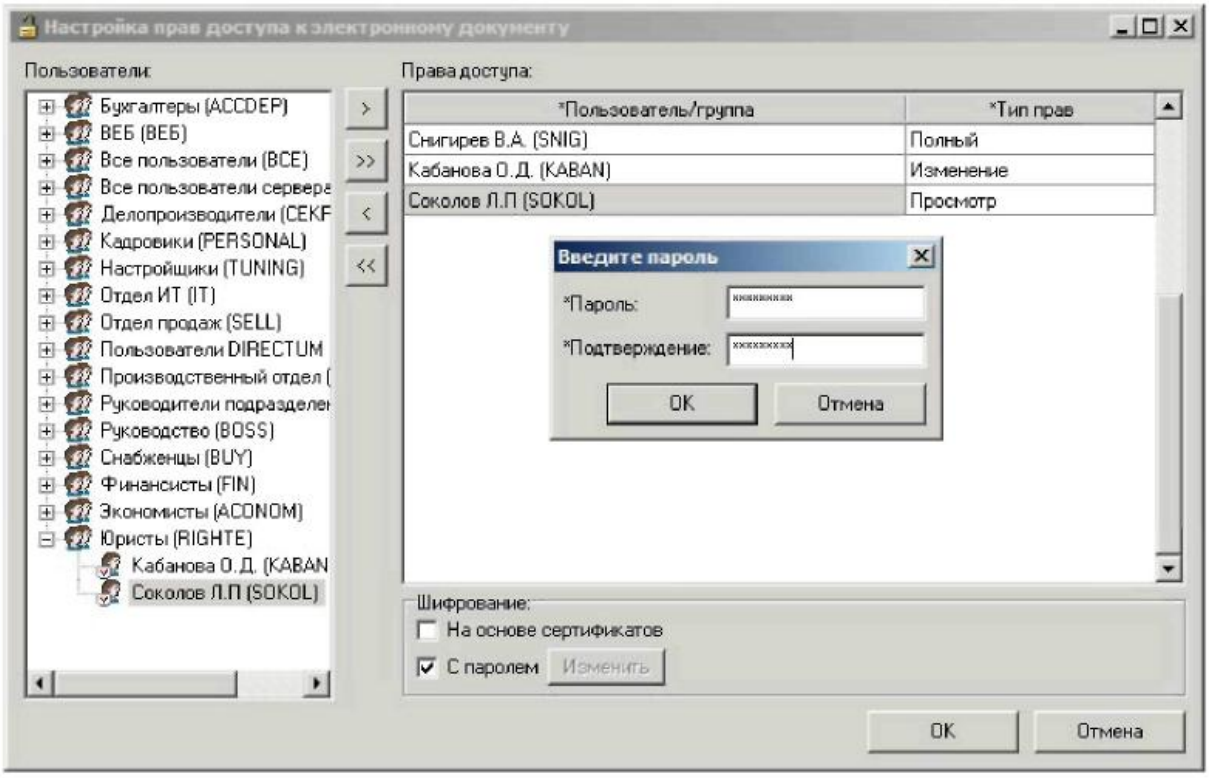

Рисунок 3.1 – Встановлення прав доступу

Шифрування на основі сертифікатів дозволяє забезпечити більше високий ступінь обмеження доступу до тексту документа. Використаються несиметричні алгоритми шифрування на основі відкритих і закритих ключів. Для їхньої реалізації в тому числі можуть застосовуватися сертифіковані ФСБ засобу крипто захисту (наприклад, КриптоПро).

Такий підхід має ряд переваг у порівнянні із шифруванням паролем: немає необхідності запам'ятовувати пароль і передавати його по відкритих каналах, складніше втратити доступ до документа. Цей варіант шифрування набагато більше стійкий і до зломів методами соціальної інженерії. Із шифруванням на основі паролів небезпека такого злому існує, тому що користувачі навряд чи будуть придумувати різні паролі для різних документів, і, довідавшись пароль для доступу до одного документа, можна буде з великою ймовірністю успішного результату застосувати його й для іншого.

4.2.3 Забезпечення дійсності документів

Забезпечення дійсності паперових документів звичайно полягає в їхньому підписанні відповідальними посадовими особами й проставлянні печатки. Аналогом підпису й печатки електронного документа служить електронно-цифровий підпис (ЕЦП). Закон Російської федерації № 1-ФЗ “Об электронной цифровой подписи”, прийнятий в 2002 році, у достатній мері визначає можли-

вість використання ЕЦП усередині організації для підтвердження дійсності документів.

Повноцінне використання ЕЦП буде здійснюватися тільки в тому випадку, якщо на підприємстві діє система електронного документообігу, тобто документи реєструються, розсилаються, узгоджуються, вивчаються в електронному виді. А тому що закон “Об электронной цифровой подписи” не пред'являє особливих вимог до використання ЕЦП у рамках корпоративної інформаційної системи, більшість внутрішніх документів організації можуть використатися тільки в електронному виді (виключенням є кадрові накази, з якими співробітники повинні бути ознайомлені під особистий розпис).

У системі DIRECTUM для підписання документа в користувача повинен бути зареєстрований сертифікат відкритого ключа (що збігає із ключем для шифрування або інший). Секретний закритий ключ перебуває тільки в його власника й недоступний іншим користувачам; відповідальність за його схоронність несе сам власник ключа.

Документ може бути підписаний одним або декількома користувачами. Під час підписання, як й у випадку із шифруванням документів, можуть застосовуватися сертифіковані засоби криптозахисту.

Підписана версія документа не може бути змінена навіть адміністратором, а несанкціоновано й безслідно підмінити текст документа неможливо навіть при наявності прямого доступу до бази даних, тому що для цього буде потрібно доступ до закритого ключа користувача. При необхідності, можна створити нову версію документа й відредагувати її.

3.2.4 Протоколювання дій користувачів

У випадку виникнення ситуацій непередбачуваної зміни тексту або картки документа, його видалення, доступу до документа користувачів, що не мають на те права, більшу допомогу робить історія роботи з документом. Функція ведення цієї історії є обов'язковою для систем електронного документообігу. В DIRECTUM робота всіх користувачів протоколюється. В історію записуються операції перегляду, зміни, створення, експорту й імпорту документів, призначення прав на доступ до них і т.д. Протоколюється робота із записами довідників. В історії фіксується тип операції, дата й час її здійснення, ім'я користувача й інша інформація.

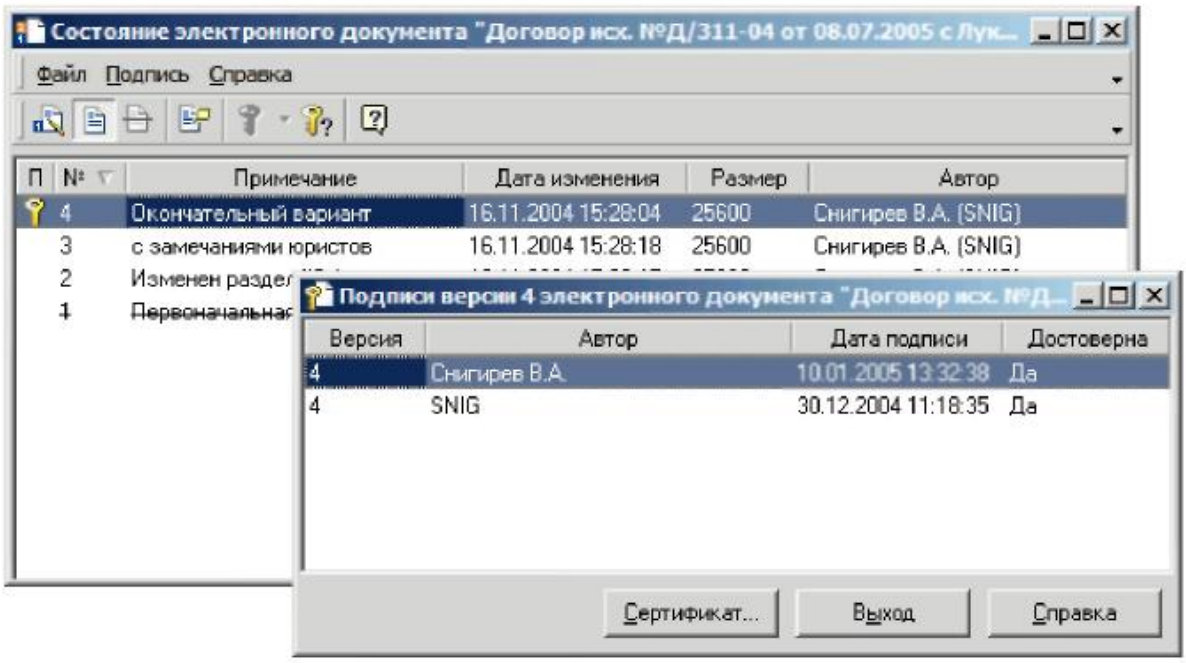

Рисунок 3.2 – Підписування версії документа

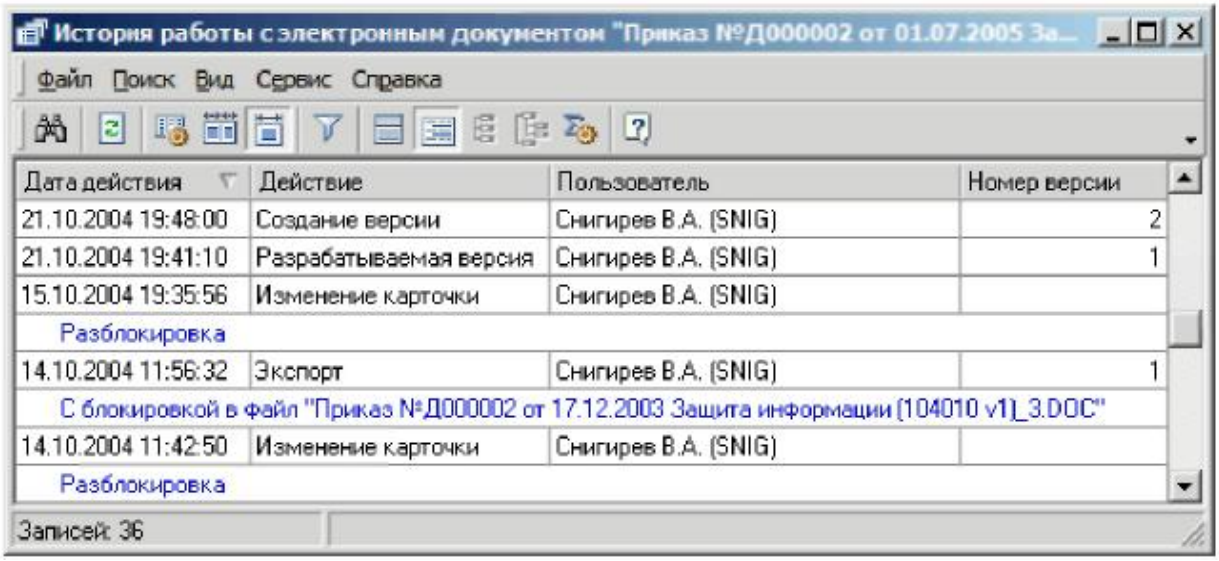

Рисунок 3.3. Протокол дій користувачів

Таким чином, система DIRECTUM вирішує всі основні проблеми, пов'язані з безпекою в умовах дії системи електронного документообігу. Забезпечується висока схоронність документів за рахунок зберігання в базі даних SQL-сервера, розмежування прав доступу, забезпечення шифрування текстів документів, роботи з ЕЦП сертифікованими засобами криптографічного захисту, протоколювання роботи всіх користувачів системи з усіма її об'єктами.

У сукупності із загальносистемним захистом програмно-апаратних засобів організації (захищені канали зв'язку, шифрування носіїв і т.п.) і ретельно продуманими організаційно-профілактичними мірами (обмеження фізичного доступу до сховищ, пристроям печатки, знімним носіям інформації, регулярне

резервне копіювання, захист від вірусів і т.ін.) система DIRECTUM забезпечує високий рівень схоронності й конфіденційності документів організації.

4.3 Реалізація політики безпеки в СЕД “Megapolis™. Документообіг”

“Megapolis™. Документообіг” [11] є комплексним програмним рішенням для створення систем управління документами та автоматизації ділових процесів. Система охоплює всі етапи життєвого циклу документів – від підготовки проектів до організації архівного зберігання документів із забезпеченням функцій електронного архіву та електронного цифрового підпису.

Система має модулі, що орієнтовані на автоматизацію традиційних вітчизняних процесів діловодства та контролю виконавчої дисципліни, характеризується відкритістю, високим рівнем розширення та адаптації і може успішно використовуватися в різних структурах – від комерційних компаній до державних органів влади.

У серпні 2006 року комплексне програмне рішення “Megapolis™. Документообіг” отримало Диплом переможця Всеукраїнського конкурсу-виставки “Кращий вітчизняний товар 2006 року” у номінації “Розробка інформаційних систем та програмного забезпечення”

4.3.1 Загальний опис функціональності

Система “Megapolis™. Документообіг” призначена для рішення наступних задач:

- організація електронного архіву документів з наданням потужних пошукових засобів і механізмів спільної роботи з документами;
- забезпечення автоматизації складних ділових процесів в організації (workflow);
- організація єдиного інформаційного простору для організації з розподіленою структурою;
- автоматизація задач діловодства та контролю виконавчої дисципліни – функцій підготовки проектів документів, реєстрації, формування резолюцій, доведення документів до виконавців, фіксації ходу виконання, контролю виконання, автоматизація функцій ведення паперового архіву;
- організація роботи зі зверненнями громадян;
- формування різноманітної статистичної й аналітичної звітності.

Застосування системи “Megapolis™.Документообіг” для рішення цих задач дає наступні результати:

- в організації формується централізована база документів та інформації про них, яка доступна в будь-який момент;
- зменшується час на виконання рутинних операцій, особливо щодо пошуку документів та зв'язаної з ними інформації;
- керівництво організації одержує своєчасне й об'єктивне інформування про стан виконання документів, рішень і окремих доручень;

• значно знижується кількість прострочених документів за рахунок організації роботи відповідальних осіб і виконавців, за рахунок зменшення терміну перебування документів у виконавців;

• збільшується прозорість документообігу, можливість його оптимізації;

• значно прискорюється робота співробітників загального відділу та секретарів підрозділів і служб керівників, підвищується оперативність технологічної обробки документів;

• частка документів, що ведуться у паперовій формі, зменшується за рахунок поступового впровадження електронної форми для документів внутрішнього призначення, а також за рахунок виключення деяких технологічних документів/

4.3.2. Склад системи

Система побудована в триланковій архітектурі “клієнт - сервер застосувань - сервер баз даних” з використанням платформи Megapolis™ і складається з наступних компонентів:

Базові програмні модулі (компоненти платформи):

• електронний архів;

• автоматизація ділових процесів (Workflow);

• обмін даними (Data Exchange);

• адміністрування та безпека;

Функціональні підсистеми:

• діловодство та контроль виконавчої дисципліни (діловодство та КВД);

• звернення громадян;

• підготовка документів;

• архівна справа;

Додаткові модулі:

• повнотекстовий пошук;

• штрих-кодування;

• сканування та розпізнавання;

• шифрування та електронний цифровий підпис (ЕЦП);

• Web-кліент.

4.3.3 Опис компонентів системи

Електронний архів

Підсистема “Електронний архів” є головною складовою системи як засіб збереження та централізованого доступу до сховища документів організації. Підсистема вирішує задачі групування та пошуку документів за різноманітними критеріями, організації колективної роботи.

Основні характеристики підсистеми:

• централізоване сховище типізованих документів;

• чітка самоорганізація (класифікація) документів;

- інтеграція з настільними офісними системами (MS Office);
- інтеграція із системами введення й обробки зображення (TWAIN);
- атрибутивний і повнотекстовий пошук з урахуванням морфології мови;
- підтримка версій документів;
- надійність і безпека збереження інформації;
- створення документів на основі шаблонів;
- простота настроювання робочого місця користувача.

Автоматизація ділових процесів (Workflow)

Підсистема "Автоматизація ділових процесів" призначена для забезпечення автоматизації регламентованих організаційних процедур (ділових процесів), які використовуються організацією за участю певних виконавців та часових обмежень. Одноразово ініційований в системі процес передає роботи від виконавця виконавцю за описаною послідовністю (схемою процесу).

Основні характеристики підсистеми:

- наявність візуальних засобів опису ділових процесів;
- автоматизація роботи учасників ділових процесів;
- накопичення знань про ділові процеси та їх централізація;
- спрощення доступу до складних ділових процесів;
- нотифікація учасників про хід виконання ділових процесів;
- контроль, аудит і моніторинг виконання ділових процесів.

Обмін даними

Підсистема "Обмін даними" призначена для забезпечення функціонування системи в розподіленому середовищі, а саме в середовищі з територіально віддаленими серверами даних.

Основні характеристики підсистеми:

- імпорт із зовнішніх джерел даних і експорт даних системи в зовнішні джерела;
- засоби перетворення даних;
- транспорт даних по різноманітних каналах з підтримкою гарантованої доставки.

Адміністрування та безпека

Підсистема "Адміністрування та безпека" призначена для гарантування надійності збереження інформації, її актуальності та достовірності, забезпечення надійності бази даних та її готовності до роботи. Поняття "користувача", "групи користувачів", "домену" та "прав" не відрізняються від відповідних понять операційної системи. Завдяки цьому, адміністрування системи може бути інтегроване з загальним адмініструванням в мережі організації. Функції безпе-

ки системи відповідають вимогам нормативно-правової бази України у галузі захисту інформації.

Основні характеристики підсистеми:

- ведення доменів, користувачів і груп користувачів;
- інтеграція із системою безпеки операційної системи;
- розподіл прав доступу до інформаційних і функціональних ресурсів;
- протоколювання дій користувачів;
- можливість розширення і настроювання підсистеми.

Діловодство та контроль виконавчої дисципліни

Підсистема "Діловодство та КВД" призначена для автоматизації сформованих в установах традиційних процесів діловодства із забезпеченням організаційних та технологічних засад для переходу до електронного документообігу. Підсистема здійснює підтримку традиційного паперового діловодства, сучасних технологій електронного документообігу, а також змішаного паперово-електронного документообігу із застосуванням технологій штрих-кодування, сканування та розпізнавання.

Основні характеристики підсистеми:

- реєстрація вхідних, вихідних, внутрішніх документів; попередній розгляд, повна реєстрація інформації, передача документів виконавцям;
- функції діловодів підрозділів (отримання документів, внутрішній контроль, реєстрація внутрішніх документів);
- контроль виконавчої дисципліни (ведення резолюцій, ходу виконання, перегляд інформації у різних розрізах);
- формування різноманітної статистичної та аналітичної звітності.

Звернення громадян

Підсистема "Звернення громадян" призначена для підвищення рівня опрацювання звернень громадян шляхом автоматизації реєстрації надходження звернень, призначення виконавців та визначення термінів виконання резолюцій.

Підготовка документів

Підсистема "Підготовка документів" призначена для надання автоматизованих засобів підготовки проектів документів із використанням шаблонів, автоматизації процесів узгодження та підписання документів.

Основні характеристики підсистеми:

- централізоване ведення єдиної бази шаблонів всіх видів документів організації;
- контроль ведення версій проектів документів;
- збереження даних у електронному архіві;

• автоматизовані засоби узгодження/підписання проектів документів;

• інтеграція з механізмами штрих-кодової ідентифікації паперових копій документів.

Архівна справа

Підсистема “Архівна справа” призначена для автоматизації процесів архівного зберігання паперових копій документів, ведення та обліку архівних справ, підтримки процесів підготовки та передачі документів до паперового архіву організації.

Основні характеристики підсистеми:

• ведення номенклатури справ підрозділу;

• ведення пунктів номенклатури справ;

• формування зведеної номенклатури;

• затвердження зведеної номенклатури справ;

• підтримка стану номенклатури;

• формування справ та томів справ;

• формування опису справи;

• формування описів справ для передачі справ у архівний підрозділ;

• формування зведених описів справ для передачі в довгостроковий архів;

• підтримка роботи з архівом - видача справ (томів), формування карток-замінників, формування і "реєстрація" запитів на копіювання документів зі справ.

Основні переваги системи

Переваги, які надаються системою “Megapolis™. Документообіг”, обумовлені унікальними властивостями цього продукту:

• побудова на платформі Megapolis™;

• єдиний інформаційний простір і безшовна інтеграція з іншими інформаційними системами (“Управління персоналом”, “Бухгалтерія” і т.д.);

• модульна побудова системи, і, як наслідок – легка модернізація, підтримка і нарощування функціональності;

• відкритий програмний код;

• забезпечення рівня гарантій Г-2 у сфері захисту інформації (НД ТЗІ 2.5-004-99);

• реляційне сховище документів;

• промисловий рівень надійності системи, цілісності і несуперечності даних, постійна готовність до роботи;

• висока швидкість роботи при великих обсягах даних;

• незалежність використання СКБД (Oracle, MSSQL) і єдина мова доступу до даних;

• наявність готової прикладної функціональності;

- потужні засоби розмежування прав доступу до функцій і даних системи;
- повне протоколювання дій користувачів;
- інтеграція із системою безпеки MS Windows;
- інтеграція із засобами шифрування та електронного цифрового підпису;
- обмін даними на основі XML;
- імпорт даних з довільних джерел, експорт у будь-які формати даних.

3.3.4 Аналіз експертного висновку на відповідність вимогам ТЗІ

Комплекс засобів захисту інформації від несанкціонованого доступу системи "Megapolis™. Документообіг" версія 1.1.0.8.

Розмежування та контроль доступу до інформаційних ресурсів системи "Megapolis™. Документообіг". Відповідає вимогам НД з ТЗІ в обсязі функцій, зазначених у технічному завданні, сукупність яких визначається функціональним профілем КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ЦО-1, ДС-1, ДР-1, ДЗ-2, ДВ-1, НР-2, НИ-1, НО-1, НЦ-1, НТ-2 з рівнем довіри Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99 [7].

Аналіз функціонального профілю захисту

Критерії конфіденційності. Для того, щоб КС могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної КС повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

Довірча конфіденційність. Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

КД-2 – базова довірча конфіденційність:

Політика довірчої, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача і захищеного об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфі-

денційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

Необхідною умовою є НИ-1.

Адміністративна конфіденційність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління.

КА-2 – базова адміністративна конфіденційність:

Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

Необхідними умовами є НО-1 та НИ-1.

Повторне використання об'єктів. Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

КО-1 – повторне використання об’єктів:

Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Критерії цілісності. Для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкіт, цілісність при обміні.

Довірча цілісність. Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ЦД-1 – мінімальна довірча цілісність:

Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

Необхідною умовою є НИ-1.

Адміністративна цілісність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

ЦА-1 – мінімальна адміністративна цілісність:

Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

Необхідними умовами є НО-1 та НИ-1.

Відкіт. Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкотити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкіт.

ЦО-1 – обмежений відкіт:

Політика відкоту, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкотити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Необхідною умовою є НИ-1.

Критерії доступності. Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Стійкість до відмов. Стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій або КС в цілому) після відмови її компонента. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість функціонування КС в залежності від кількості відмов і послуг, доступних після відмови.

ДС-1 – стійкість до обмежених відмов:

Розробник повинен провести аналіз відмов компонентів КС Політика стійкості до відмов, що реалізується КЗЗ, повинна визначати множину компонентів КС, до яких вона відноситься, і типи їх відмов, після яких КС в змозі продовжувати функціонування.

Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги.

Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг, а має в гіршому випадку проявлятися в зниженні характеристик обслуговування.

КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного компонента.

Необхідною умовою є НО-1.

Використання ресурсів. Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

ДР-1 – квоти:

Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу.

Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

Необхідною умовою є НО-1.

Гаряча заміна. Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні даної послуги ранжируються на підставі повноти реалізації.

ДЗ-2 – модернізація:

Політика гарячої заміни, що реалізується КЗЗ, повинна визначати політику проведення модернізації КС.

Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію (upgrade) КС. Модернізація КС не повинна призводити до необхідності ще раз проводити інсталяцію КС або до переривання виконання КЗЗ функцій захисту.

Необхідною умовою є НО-1.

Відновлення після збоїв. Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

ДВ-1 – ручне відновлення:

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС.

Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування.

Необхідною умовою є НО-1.

Критерії спостереженості. Для того, щоб КС могла бути оцінена на предмет відповідності критеріям спостереженості, КЗЗ оцінюваної КС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції. Спостереженість забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача

Реєстрація. Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю,

складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

НР-2 – захищений журнал:

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки.

Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Необхідними умовами є НИ-1 та НО-1.

Ідентифікація і автентифікація. Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

НИ-1 - Зовнішня ідентифікація і автентифікація:

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ.

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача.

Розподіл обов'язків. Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

НО-1 – виділення адміністратора:

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції.

Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

Необхідною умовою є НИ-1.

Цілісність комплексу засобів захисту. Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

НЦ-1 – КЗЗ з контролем цілісності:

Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ.

В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Необхідними умовами є НР-1 та НО-1.

Самотестування. Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

НТ-2 – самотестування за запитом:

Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження.

Аналіз рівня гарантій Г-2

Критерії гарантій включають вимоги до архітектури комплексу засобів захисту (КЗЗ), середовища розробки, послідовності розробки, середовища функціонування, документації і випробувань КЗЗ. В цих критеріях вводиться сім рівнів гарантій, які є ієрархічними. Вимоги викладаються за розділами. Для того, щоб комп’ютерна система (КС) одержала рівень гарантій Г-2, повинні бути задоволені наступні вимоги.

Архітектура:

- Вимоги до архітектури забезпечують гарантії того, що КЗЗ у змозі повністю реалізувати політику безпеки.
- КЗЗ повинен реалізовувати політику безпеки. Всі його компоненти повинні бути чітко визначені

Середовище розробки:

Вимоги до середовища розробки забезпечують гарантії того, що процеси розробки і супроводження оцінюваної КС є повністю керованими з боку Розробника.

Процес розробки:

Розробник повинен визначити всі стадії життєвого циклу КС, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги

Керування конфігурацією:

Розробник повинен розробити, запровадити і підтримувати в робочому стані документовані методики щодо керування конфігурацією КС на всіх стадіях її життєвого циклу. Система керування конфігурацією повинна забезпечувати керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією повинна гарантувати постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ

Послідовність розробки:

Вимоги до процесу проектування (послідовності розробки) забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис КС і реалізація КС точно відповідає вихідним вимогам (політиці безпеки).

Функціональні специфікації (політика безпеки):

Відповідність політиці безпеки – показ.

Функціональні специфікації повинні включати модель політики безпеки.

Проект архітектури:

Відповідність моделі політики безпеки – показ.

На стадії розробки ескізного проекту Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використовувані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ повинні бути описані в термінах винятків, повідомлень про помилки і кодів повернення

Детальний проект - показ

Середовище функціонування:

Вимоги до середовища функціонування забезпечують гарантії того, що КС поставляється Замовнику без несанкціонованих модифікацій, а також інсталюється і ініціюється Замовником так, як це передбачається Розробником.

Розробник повинен представити засоби інсталяції, генерації і запуску КС, які гарантують, що експлуатація КС починається з безпечного стану. Розробник повинен представити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску

Документація:

Вимоги до документації є загальними для всіх рівнів гарантій.

У вигляді окремих документів або розділів (підрозділів) інших документів Розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ, настанови адміністратору щодо послуг безпеки, настанови користувача щодо послуг безпеки.

В описі функцій безпеки повинні бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується КЗЗ оцінюваної КС, а також самі послуги.

Настанови адміністратору щодо послуг безпеки мають містити опис засобів інсталяції, генерації і запуску КС, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску КС, опис властивостей КС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адмі-

ністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує КС.

Настанови користувачу щодо послуг безпеки мають містити інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Назва документів (розділів) не регламентується. Опис послуг безпеки може відрізнятися для користувача і адміністратора. Настанови адміністратору і настанови користувачу можуть бути об'єднані в настанови з установлення і експлуатації.

Випробування комплексу засобів захисту:

Розробник повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття

Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування

Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування

Розробник повинен усунути або нейтралізувати всі знайдені “слабкі місця” і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця ”

5 РЕАЛІЗАЦІЯ КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ MICROSOFT SQL SERVER 2005

5.1 Загальні відомості про управління доступом

5.1.1 Авторизація й автентифікація

Автентифікація — це процес перевірки права користувача на доступ до того або іншого ресурсу. Найчастіше автентифікація здійснюється за допомогою уведення імені й пароля [11].

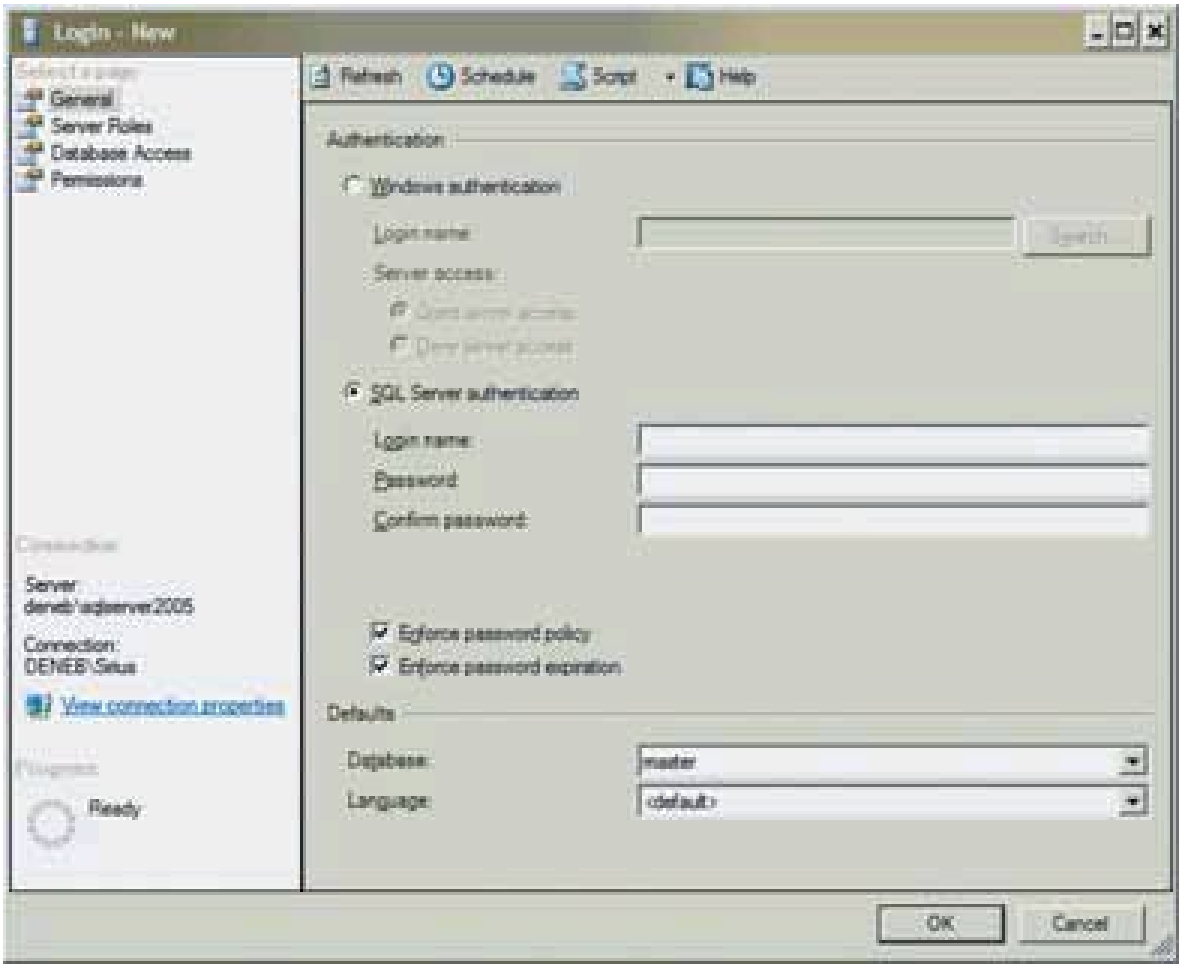

Рисунок 3.1 - Установка правил для пароля користувача

SQL Server 2005 підтримує два режими автентифікації: за допомогою Windows і за допомогою SQL Server. Перший режим дозволяє реалізувати рішення, засноване на однократній реєстрації користувача і єдиному паролі при доступі до різних додатків (Single SignOn solution, SSO). Подібне рішення спрощує роботу користувачів, рятуючи їх від необхідності запам'ятовування безлічі паролів і тим самим знижуючи ризик їхнього небезпечного зберігання

(згадаємо стикеры з паролями, наклеєні на монітори). Крім того, даний режим дозволяє використати засоби безпеки, надавані операційною системою, такі як застосування групових і доменних політик безпеки, правил формування й зміни паролів, блокування облікових записів, застосування захищених протоколів автентифікації за допомогою шифрування паролів (Kerberos або NTLM).

Автентифікація за допомогою SQL Server призначена головним чином для клієнтських додатків, що функціонують на платформах, відмінних від Windows. Цей спосіб уважається менш безпечним, але в SQL Server 2005 він підтримує шифрування всіх повідомлень, якими обмінюються клієнт і сервер, у тому числі за допомогою сертифікатів, згенерованих сервером. Шифрування також підвищує надійність цього способу автентифікації. Для облікового запису SQL Server можна вказати такий параметр, як необхідність перемінити пароль при першому з'єднанні із сервером. Якщо SQL Server 2005 працює під управлінням Windows Server 2003, можна скористатися такими параметрами облікового запису, як перевірка терміну дії пароля й локальна парольна політика Windows (рисунок 3.1).

Відзначимо такий дріб'язок, як обов'язкова вимога непустого пароля користувача sa - як не дивно, порожній пароль даного облікового запису є досить розповсюдженим проявом безтурботності адміністраторів баз даних (і самою улюбленою лазівкою для викрадачів корпоративних даних).

5.1.2 Схеми, що не мають відносини до користувачів

От уже не перший десяток років принцип розподілу прав доступу до об'єктів баз даних у більшості серверних СУБД заснований на наявності в кожного об'єкта бази даних користувача-власника, що може надавати іншим користувачам права доступу до об'єктів бази даних. При цьому набір об'єктів, що належать тому самому користувачеві, називається схемою. Даний спосіб володіння об'єктами створював певні незручності при супроводі додатків, що використають бази даних. Так, при звільненні співробітника, що створив об'єкти, використовувані багатьма користувачами, і видаленні відповідного облікового запису доводилося вносити зміни в серверний код (а нерідко й у код клієнтського додатка). Розуміння можливості виникнення цих проблем привело до поширення небезпечних, але простих у застосуванні способів управління обліковими записами користувачів. Аж до зберігання їхніх імен і паролів у звичайних таблицях, що різко підвищувало погрозу несанкціонованого доступу до даних і додатків.

В SQL Server 2005 концепція ролей розширена: ця СУБД дозволяє повністю відокремити користувача від схем й об'єктів бази даних. Тепер об'єкти бази даних належать не користувачеві, а схемі, що не має ніякого відношення ні до яких облікових записів і тим більше до адміністративних привілеїв. Таким чином, схема стає механізмом угруповання об'єктів, що спрощують надання користувачам прав на доступ до об'єктів.

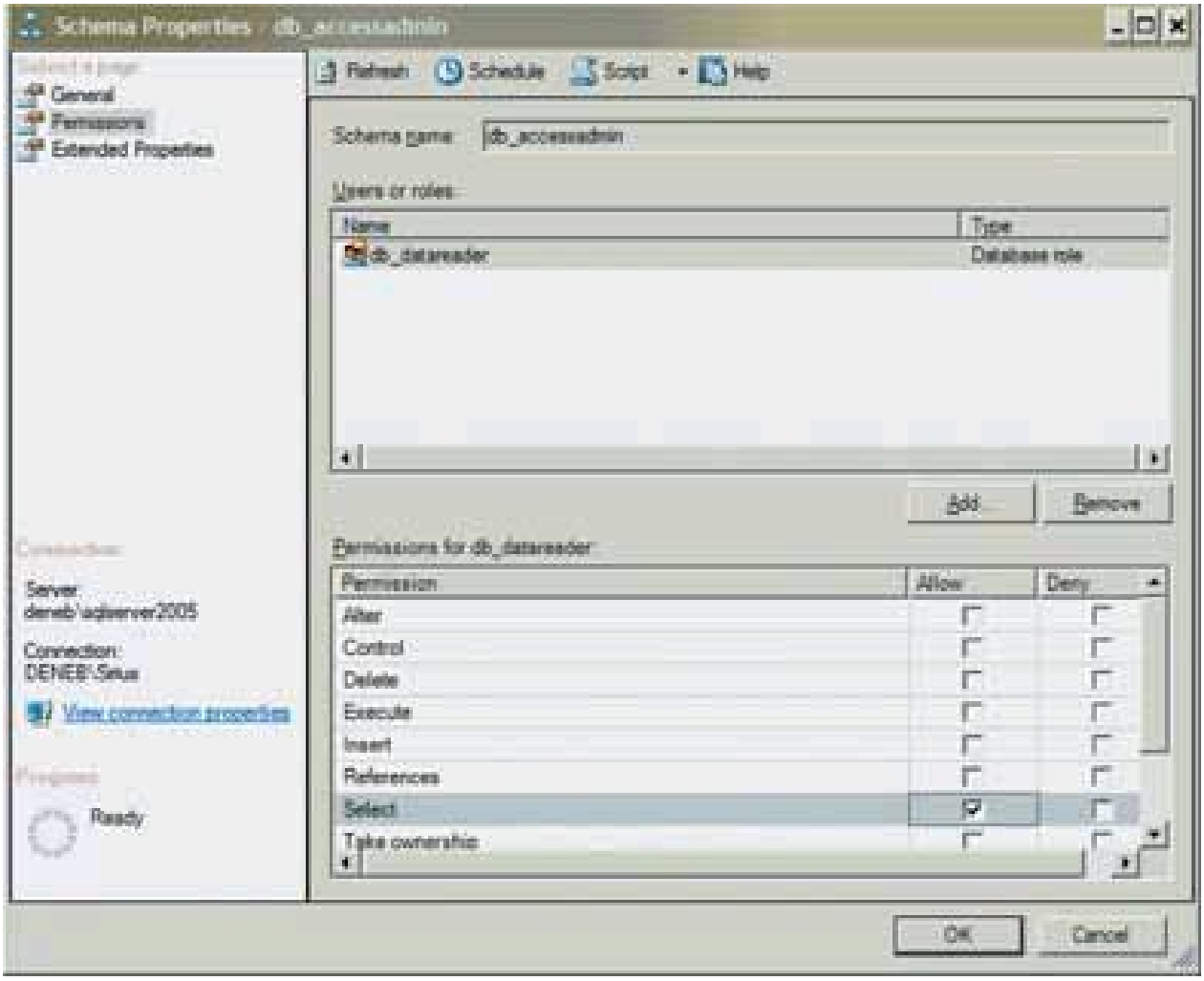

Рисунок 3.2 - Установка прав для схем даних

5.1.3 Ролі

Для спрощення управління правами доступу в більшості серверних СУБД застосовується механізм ролей - наборів прав доступу до об'єктів бази даних, що привласнює деякої сукупності користувачів. При використанні ролей управління розподілом прав доступу до об'єктів між користувачами, що виконують однакові функції й застосовують ті самі додатки, істотно спрощується:

створення ролі й однократне призначення їй відповідних прав здійснюється набагато швидше, ніж визначення прав доступу кожного користувача до кожного об'єкта. SQL Server 2005 дозволяє створювати так називані вкладені ролі, тобто привласнювати однієї ролі іншу з усіма її правами. Це спрощує управління не тільки правами користувачів, але й самими ролями, створюючи, приміром, подібні між собою групи ролей.

SQL Server 2005 також підтримує так називані ролі для додатків (application roles), які можуть використатися для обмеження доступу до об'єктів бази даних у тих випадках, коли користувачі звертаються до даних за допомогою конкретних додатків. На відміну від звичайних ролей, ролі для додатків, як правило, неактивні й не можуть бути привласнені користувачам. Їхнє застосування виявляється зручним у тому випадку, коли вимоги безпеки єдині для всіх користувачів, при цьому не потрібен аудит або інша реєстрація діяльності конкретних користувачів у базі даних.

5.2 Рекомендації з управління доступом

Нижче треба ряд нескладних рекомендацій, що стосується застосування засобів управління доступом при створенні й розгортанні рішень на основі SQL Server 2005.

5.2.1 Загальні принципи застосування схем і ролей

Одним з обов'язкових етапів проектування баз даних повинне бути детальне визначення способів доступу до об'єктів бази даних. Зокрема, на цьому етапі необхідно визначити, яким образом використати схеми для угруповання об'єктів бази даних з погляду доступу до них, які ролі створити, визначити можливі групи користувачів і ролі, які треба їм привласнити. Крім того, на цьому ж етапі важливо ухвалити рішення щодо тім, як будуть використатися подання й збережені процедури для забезпечення безпечного доступу до даних (наприклад, для обмеження безпосереднього доступу до таблиць).

Останнім часом настійно рекомендується застосовувати ролі у всіх рішеннях (як було сказано вище, це помітно знижує витрати на процес управління правами доступу й внесення в них змін), а у випадку наявності користувачів, що мають частково співпадаючі набори прав доступу, рекомендується застосовувати вкладені ролі. Для визначення прав доступу й правил вкладеності ролей варто розділити користувачів на групи з різними правами доступу й зрозуміти,

чи можна сформулювати правила вкладеності груп, а потім відбити ці відомості в проектованих ролях.

Потрібно також проаналізувати вимоги до прав доступу, пропоновані клієнтськими додатками, і врахувати ці вимоги при проектуванні ролей і створенні схем. Не коштує при цьому забувати й про те, що списки користувачів і ролей треба не тільки створити один раз, але й постійно актуалізувати. Крім питань управління доступом у клієнтських додатках, рекомендується приділити увага й керуванню доступом у різних службах SQL Server.

5.2.2 Управління доступом у службах звітів

При застосуванні служб звітів (Reporting Services) необхідно окремо подбати про правила доступу до об'єктів бази даних для користувачів, що застосовують додатки, що звертаються до цих служб. Так, зазначеної категорії користувачів повинні бути доступні як самі описи звітів, так і ті об'єкти бази даних, на підставі яких ці звіти генеруються, і в цьому випадку найбільш доречне створення окремої ролі, що володіє зазначеними правами. Варто помітити, що за замовчуванням служби звітів використають служби Internet Information Services (IIS) і засобу безпеки Windows для автентифікації користувачів на сервері звітів. Даний режим уважається найбільш безпечним, оскільки може дозволити заборонити анонімний доступ до web-додатків, що виконується під управлінням IIS.

Відзначимо, що сервіси звітів можуть виконуватися в режимі Integrated Security. Але в цьому випадку вони виконують код ряду компонентів з тими ж привілеями, що й у користувача, що згенерував звіт, а це дозволить користувачеві, що виконує звіт, одержати більше високі привілеї, ніж йому покладені. Тому даний режим не рекомендується застосовувати разом зі службами звітів.

5.2.3 Управління доступом у службах повідомлень

Служби повідомлень (Notification Services) виконуються від імені власного облікового запису, що, з одного боку, повинна мати певні права для забезпечення доставки повідомлень, з іншого боку, зазначений набір прав повинен бути мінімально необхідним (як мінімум, такий обліковий запис не повинна входити в групу Administrators).

Відзначимо, що для служб повідомлень існують спеціальні ролі - NSEventProvider, NSGenerator, NSDistributor, які варто привласнювати обліко-

вим записам, відповідальним за провайдери, генератори й механізми розсилання, а також роль NSRunService, що включає в себе три перераховані ролі й застосовується в тім випадку, якщо всі складові частини служб повідомлень виконуються усередині одного ядра бази даних.

5.2.4 Управління доступом в інтеграційних службах

Для управління доступом в інтеграційних службах в SQL Server 2005 уведені нові ролі: db_dt sadmin, db_dt sltuser й db_dtsoperator. Вони дозволяють здійснювати контроль доступу до пакетів інтеграційних служб, що зберігаються в базі даних msdb.

5.2.5 Управління доступом у службах реплікації

Для управління доступом у службах реплікації SQL Server 2005 була створена нова модель безпеки цих служб, що дозволяє більш гнучко управляти обліковими записами агента реплікації (Replication Agent). Тепер кожен агент реплікації може виконуватися під власним обліковим записом, що дозволяє наділити кожного агента саме тими правами, які потрібні для його функціонування, без присвоєння надлишкових привілеїв. При цьому, якщо сервери, що беруть участь у процесі реплікації, перебувають в одному домені, для зазначених облікових записів рекомендується використати автентифікацію Windows.

Для управління доступом до самих публікацій рекомендується для кожного агента використати списки публікацій - Publication Access Lists, що включають облікові записи користувачів. Окремо відзначимо необхідність захисту папки файлової системи Snapshot, що містить репліковані дані, і надавати агентам, що не здійснюють запис у цю папку, таким як Replication Merge Agent й Replication Distribution Agent, доступ тільки в режимі читання.

5.2.6 Управління доступом для SQL Server Agent

Агент SQL Server Agent повинен виконуватися від імені облікового запису Windows, що володіє роллю sysadmin, але не належить групі Administrators й має дозвіл на збільшення квот пам'яті для процесу. Сам SQL Server Agent повинен виконуватися як служба операційної системи, протоколюватися як сервіс. Крім того, можна створити спеціальну проксі-запис й асоціювати її з відповідними правами Windows для доступу до зовнішніх ресурсів.

Для управління службою SQL Server Agent можна використати утиліту Surface Area Configuration (рисунок 3.3).

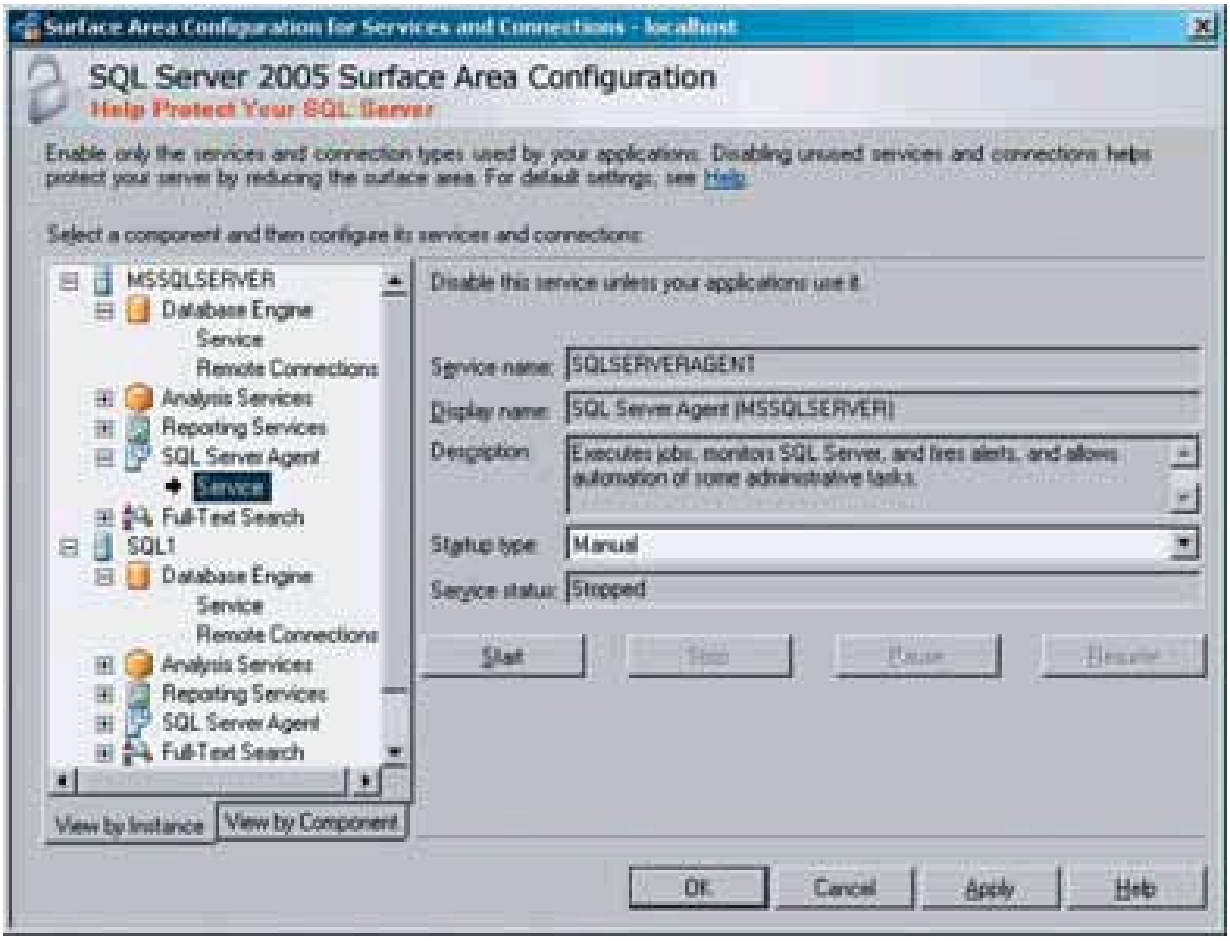

Рисунок 3.3 - Управління службою SQL Server Agent

5.2.7 Управління доступом для Database Mail

Database Mail - це новий компонент SQL Server 2005, призначений для підтримки протоколу SMTP (Simple Mail Transport Protocol). Для управління доступом до нього рекомендується створювати набудовують профілі, що, що дозволяють указати, яким образом користувачі бази даних msdb мають доступ до даного профілю (самим користувачам варто привласнити роль DatabaseMailUserRole бази даних msdb). Для управління службою Database Mail можна також використати утиліту Surface Area Configuration (рисунок 3.4).

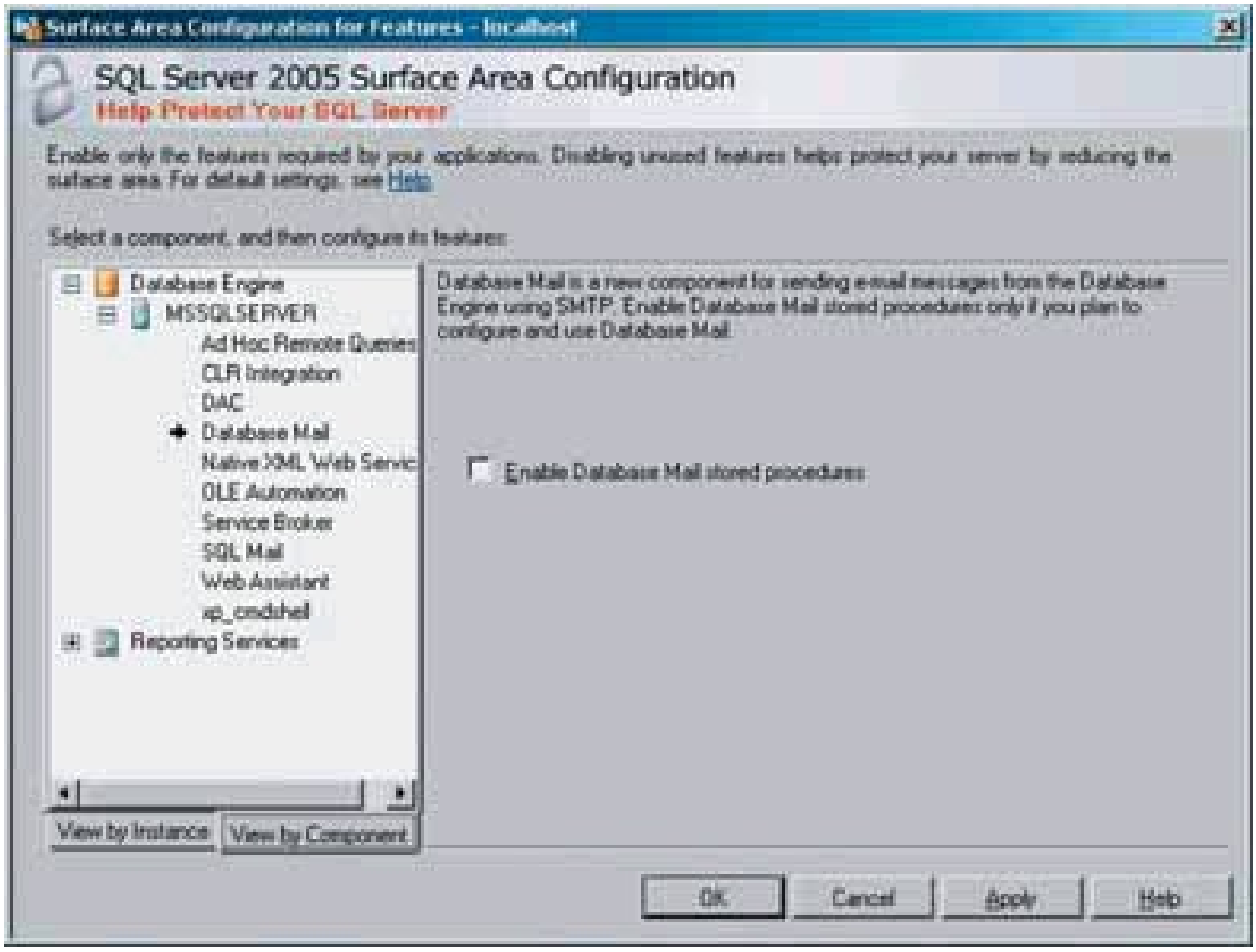

Рисунок 3.4 - Управління службою Database Mail

5.2.8 Управління доступом до бази даних за допомогою протоколу HTTP

Оскільки HTTP-доступ є одним з найпоширеніших способів атак на додатки ззовні, варто дозволити доступ до HTTP Endpoints тільки тих користувачам або групам, яким він дійсно необхідний. Крім того, на сервері баз даних варто відключити обліковий запис Windows Guest, оскільки вона дозволяє користувачам підключатися до комп'ютера без уведення пароля. У черговий раз нагадаємо: доступ до SQL Server через Інтернет повинен здійснюватися тільки за допомогою брандмауера.

5.3. Виконання коду з мінімальними привілеями

5.3.1 Установки за замовчуванням

Один з базових принципів створення безпечних додатків - принцип надання мінімальних привілеїв, необхідних для рішення поставленого завдання, -

в SQL реалізований у набагато більше строгих настроюваннях за замовчуванням, ніж у попередніх версіях. Так, у новій версії SQL Server за замовчуванням відключена значна кількість функцій, таких як застосування Microsoft .NET Framework у ядрі СУБД, функції SQL Service Broker Network Connectivity, доступ до аналітичних служб за допомогою протоколу HTTP. Такі служби, як SQL Server Agent, Data Transformation Services і засобу повнотекстового пошуку, після установки сервера вимагають ручного запуску.

5.3.2 Управління контекстом виконання коду

SQL Server 2005 дозволяє вказати контекст безпеки, у якому будуть виконуватися ті або інші оператори програмного модуля, а саме облікового запису, що використається при перевірці дозволів на об'єкти, на які посилається процедура або функція. Це може бути, наприклад, обліковий запис користувача, що викликав процедуру, або обліковий запис користувача, що створив процедуру, або ж інший обліковий запис.

Одне з нововведень SQL Server 2005, що реалізує принцип мінімальних привілеїв, дозволяє виконувати збережені процедури й функції, обумовлені користувачем, із правами іншого користувача. Для цієї мети є оператор EXECUTE AS. Він дозволяє більш гнучко управляти правами, надаваними виконує коду, що, і не зв'язувати їх із правами самого користувача. Зазначена функціональність може застосовуватися для безпечного управління правами користувачів. Так, рішення такої часто, що зустрічається завдання, як надання доступу до процедури без надання доступу до таблиці, що використає дана процедура, вирішується за допомогою оператора EXECUTE AS без необхідності надання користувачам процедури додаткових привілеїв. Конструкція EXECUTE AS, що вказує при створенні відповідного об'єкта бази даних, задає користувальницький обліковий запис, що SQL Server буде використати для перевірки прав доступу до об'єктів, використовуваним у коді збереженої процедури або користувальницької функції. У результаті код, виконання якого ініційовано користувачем, виконується так, ніби користувач зареєструвався під іншим обліковим записом. Використання конструкції EXECUTE AS дозволяє виключити циклічне призначення й перевірку прав доступу при виконанні конструкцій SELECT, INSERT, UPDATE, DELETE й EXECUTE, а також відкриття безпосереднього доступу до ряду об'єктів бази даних.

5.3.3 Рівні безпеки виконання коду

Виконання .NET-коду в ядрі СУБД, будучи засобом розширення функціональності сервера, являє собою потенційну уразливість. Тому при завантаженні зборки воно вимагає вказівки одного із трьох рівнів безпеки: SAFE (доступ до зовнішніх ресурсів не допускається), EXTERNAL_ACCESS (допускається доступ до файлів, мережним ресурсам, реєстру, змінним оточення), UNSAFE (доступ до всіх ресурсів, у тому числі до некерованого коду). Якщо зборка в процесі роботи вийде за зазначені при її завантаженні параметри безпеки, Common Language Runtime згенерує виключення, і виконання коду зборки припиниться.

5.3.4 Деякі рекомендації

Нижче ми обговоримо способи забезпечення безпеки при використанні керованого коду. У першу чергу, підтримка застосування Microsoft .NET Framework у ядрі СУБД повинна бути включена тільки в тих випадках, коли використання керованого коду в додатку дійсно необхідно. Крім того, з метою збереження стабільності роботи самої СУБД керованому коду варто привласнювати мінімально необхідний рівень привілеїв, а користувальницький код повинен виконуватися в контексті користувальницької сесії, що його викликала, і із привілеями, необхідними для даного контексту, - у противному випадку з користувальницького коду можливий неавторизований доступ до даних. Не варто нагадувати, що користувальницький код не повинен звертатися до ресурсів за межами сервера.

5.4 Шифрування трафіка й даних

5.4.1 Убудовані засоби шифрування й підтримувані алгоритми

SQL Server 2005 містить убудовані засоби шифрування, цифровому підпису й верифікації даних за допомогою симетричних ключів (алгоритми шифрування RC4, RC2, DES, AES) і асиметричних ключів (алгоритм RSA). Весь трафик між клієнтом і сервером за замовчуванням шифрується із застосуванням протоколів IP Security (IP SEC) і Secure Sockets Layer (SSL), причому подібна функціональність доступна у всіх редакціях продукту. SQL Server 2005 дозволяє при необхідності визначити політикові безпеки, повністю заборонний обмін

незашифрованими даними між клієнтом і сервером, що знижує ризик витоку даних, отриманих шляхом перехоплення трафіка.

Протокол SSL підтримується за допомогою інтеграції зі службами Internet Information Services (IIS) або за допомогою сервера сертифікатів, що підтримує стандарт X. 509v3 і вхідного до складу SQL Server 2005. Згенеровані сертифікати не тільки використаються для створення SSL-з'єднань - їх застосовує й SQL Service Broker.

5.4.2 Шифрування даних на рівні стовпчиків

SQL Server 2005 дозволяє здійснити захист даних на рівні стовпчиків за рахунок шифрування збереженої в них інформації. Він підтримує також шифрування самих збережених даних, повністю інтегроване з інфраструктурою управління ключами. Для цієї мети служать убудовані функції EncryptByCert, DecryptByCert, EncryptByKey, DecryptByKey, EncryptByAssym, DecryptByAssym, що дозволяють використати шифрування за допомогою сертифіката, симетричного й асиметричного ключів у коді Transact-SQL. Необхідно, проте, пам'ятати про те, що шифрування даних може привести до втрати продуктивності, тому при створенні рішень рекомендується шифрувати тільки конфіденційні дані й здійснювати тестування продуктивності готового рішення.

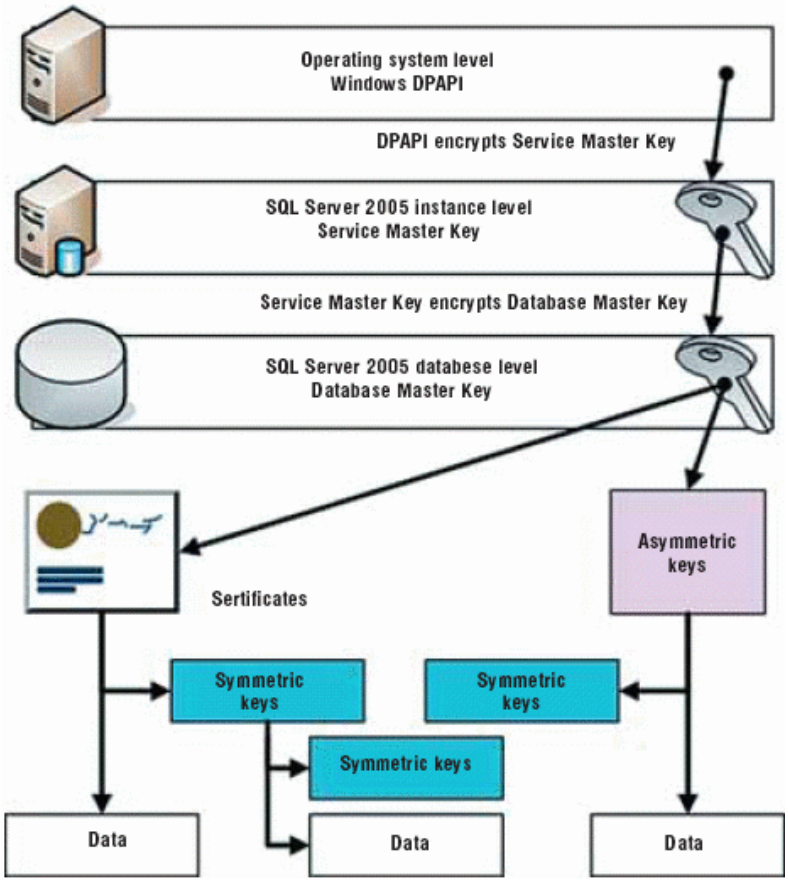

Рисунок 3.5 - Ієрархія методів шифрування в SQL Server

Здійснюючи шифрування на рівні стовпчиків, варто також розуміти, що зашифровані дані не можна сортувати, фільтрувати й індексувати, і незалежно від того, якої був тип вихідних (незашифрованих) даних, їхня зашифрована версія повинна зберігатися як VARBINARY ().

5.4.3 Шифрування даних в інтеграційних службах

В інтеграційних службах, реалізованих в SQL Server 2005, з'явився ряд нових можливостей, пов'язаних із шифруванням пакетів даних. Так, тепер доступна можливість цифрового підпису пакетів SQL Server Integration Services, що дозволяє ідентифікувати змінені пакети й забороняти їхнє завантаження. Є також можливість шифрування всього пакета із застосуванням пароля (це дозволяє запускати пакет декільком користувачам) або користувальницького ключа (що дозволяє запустити пакет тільки одному конкретному користувачеві).

Для захисту всіх об'єктів усередині пакета його можна зашифрувати цілком. Але існує й можливість вибіркового шифрування пакетів за допомогою застосування властивості пакета ProtectionLevel.

5.4.4 Шифрування даних у службах звітів

При генерації звіту служби звітів виконують запити до джерел даних, на підставі яких звіт генерується. При цьому, природно, вони використають дані про обліковий запис для доступу до цих джерел даних.

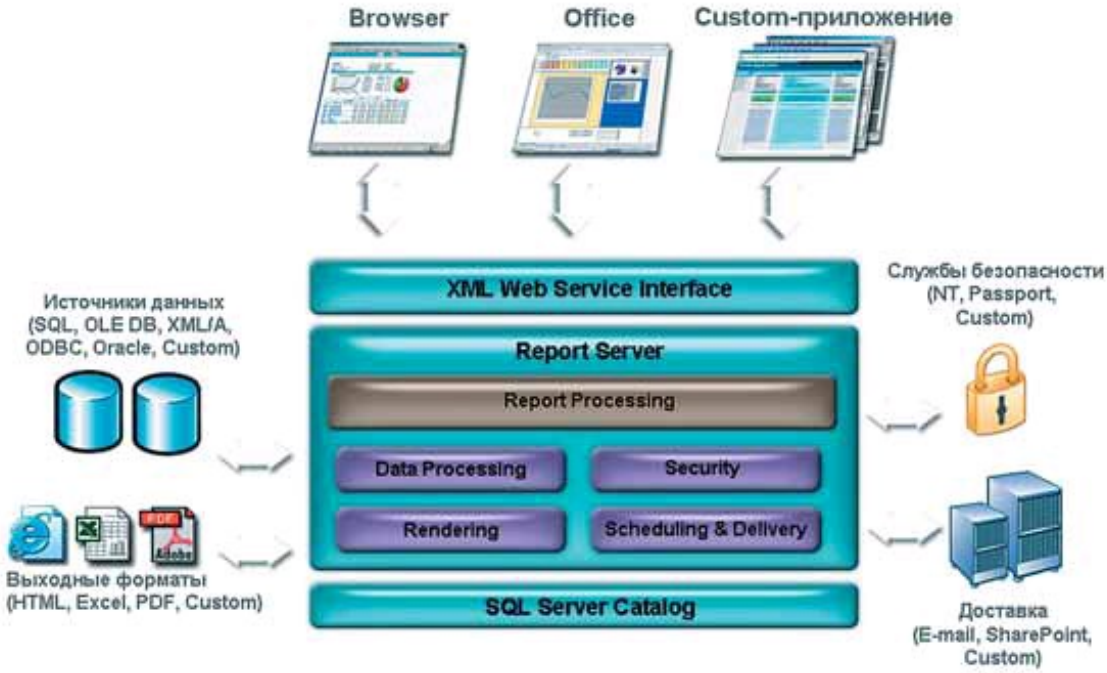

Рисунок 3.6 - Принцип роботи служб звітів

Для захисту даних про обліковий запис звичайно рекомендується використати механізми SSL, особливо у випадку, коли використаються механізми нестандартної автентифікації (custom authentication), або коли для генерації звітів використається звертання до зовнішніх джерел даних, що вимагає додаткової автентифікації. При доступі до служб звітів через Internet варто використати SSL не тільки для захисту облікових даних, але й даних самих звітів.

Настійно рекомендується зробити резервні копії ключів шифрування. Оскільки такі ключі створюються під час установки або наступної конфігурації сервера звітів, у випадку його аварії й наступного відновлення вони будуть потрібні для доступу до зашифрованих даних. Відзначимо, що клієнтські додатки, що звертаються до служб звітів, також у ряді випадків повинні забезпечити шифрування даних, для чого може бути використаний механізм Data Protection Application Programming Interface (DPAPI). Крім цього рекомендується використати мінімальний рівень привілеїв для виконання таких додатків.

5.4.5 Шифрування даних, доступних за допомогою протоколу HTTP

Надання HTTP-доступу до ядра бази даних, що дозволяє зробити дані доступними практично необмеженому числу користувачів, є одним з найцікавіших нововведень в SQL Server 2005 (рисунок 3.7).

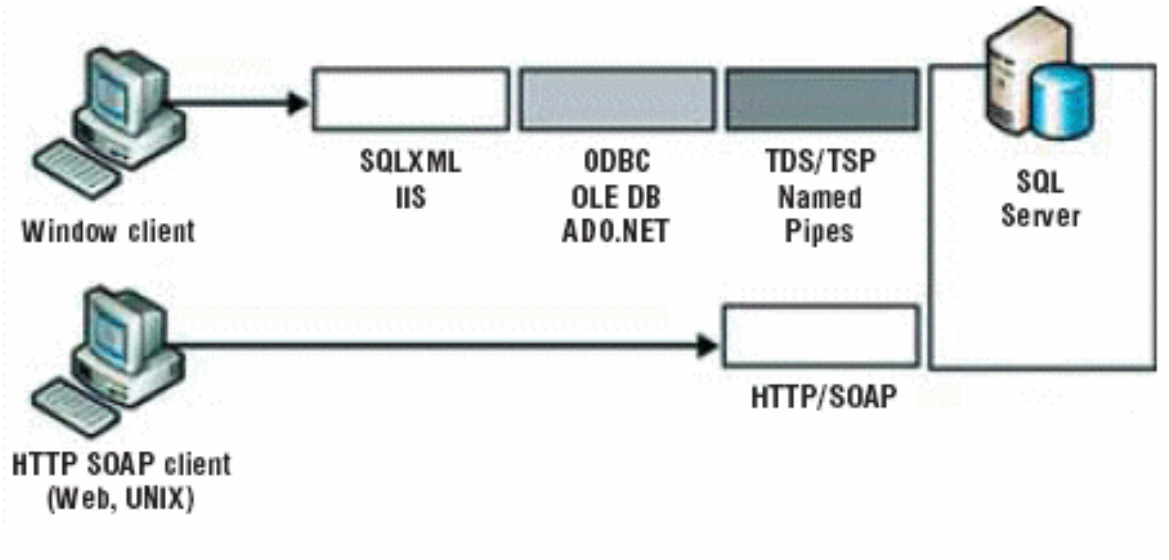

Рисунок 3.7 - Забезпечення HTTP-доступу до ядра бази даних

Однак це нововведення несе в собі й певній погрозі безпеки - адже атаки із застосуванням протоколу HTTP є сьогодні одним з найпоширеніших видів атак. Тому для захисту сервера й даних при реалізації web-служб засобами SQL Server 2005 застосовуються загальні принципи забезпечення безпеки в web-додатках й web-службах. Так, якщо планується використати web-служби для обміну конфіденційною інформацією між SQL Server і клієнтом, варто використати механізм SSL для забезпечення необхідного рівня її захисту.

В SQL Server 2005 існує можливість звертатися до web-служб, створеним засобами SQL Server 2005, із застосуванням наступних автентифікаційних механізмів: Basic, Digest, NTLM, Kerberos й Integrated (NTLM й Kerberos). Механізм автентифікації Kerberos є найбільш захищеним, тому що в ньому використаються могутніші в порівнянні з іншими механізмами алгоритми шифрування. Крім того, він здатний аутентифицировать і сервер, і клієнта, що дозволяє уникнути фармінгу - одержання конфіденційних даних клієнта із застосуванням підробленого сервера.

5.4.6 Шифрування коду збережених процедур і подань

При необхідності можна скористатися механізмами шифрування коду збережених процедур, для чого в конструкціях CREATE PROCEDURE й ALTER PROCEDURE варто використати ключове слово WITH ENCRYPTION. Є можливість шифрування коду подань - для цього в конструкції CREATE VIEW або ALTER VIEW варто використати ключове слово WITH ENCRYPTION. Подібний спосіб обмеження доступу до коду подань і процедур застосовується при впровадженні рішень на основі SQL Server з метою захисту

від несанкціонованого внесення в нього змін. При цьому вихідний код збереженої процедури або подання обов'язково варто зберегти в проекті SQL Server на випадок необхідності його модифікації в майбутньому.

5.5 Аудит і захист метаданих

5.5.1 Аудит даних і метаданих

Аудит — досить розповсюджений спосіб виявлення некоректних або неавторизованих дій користувачів, особливо користувачів, що мають надлишкові привілеї. SQL Server 2005 підтримує кілька способів підтримки аудита. Він може використати Windows Security EventLog (механізм відстеження звертань до об'єктів, використання прав, спроб автентифікації), SQL Profiler (засіб здійснення детального аудита спроб доступу до об'єктів БД).

Для здійснення аудита корисним може виявитися ще один новий механізм, що з'явився в SQL Server 2005, - тригери, пов'язані зі зміною метаданих (DDL-тригери). Створення подібних тригерів може дозволити як відслідковувати спроби зміни метаданих користувачами, так і повністю їх заборонити.

5.5.2 Приховування метаданих

У SQL Server 2005 системні об'єкти перебувають у схованій базі mssqlsystemresource, при цьому користувачам доступні подання Catalog Views для звертання до системних таблиць. Дані із цих подань фільтруються залежно від того, хто робить запит. Є й спеціальний дозвіл VIEW DEFINITION, що дозволяє обійти приховання метаданих всієї БД, схеми або конкретного об'єкта.

5.6 Основні рекомендації для адміністраторів

Незважаючи на те, що SQL Server 2005 задовольняє практично всім сучасним вимогам забезпечення безпеки, саме по собі впровадження цього продукту не захистить компанію від погроз. Питання безпеки при використанні СУБД не є чисто технологічними - проблеми з їхнім рішенням часто виникають із-за недостатньої компетентності, а те й несумлінності людей, що застосовують СУБД, що створює рішення на їхній основі або рішення, що впроваджують ці, так само як і через дії співробітників-інсайдерів, що свідомо порушують правила безпеки з метою одержання особистої вигоди. Крім того, забезпечення

«твердого» режиму безпеки найчастіше ускладнює виконання співробітниками їхніх завдань, утрудняючи доступ до необхідного для цього даним і функціям.

Нерідко вибір розумного компромісу між безпекою й доступністю функцій, додатків і даних виявляється набагато більше складним, ніж технологічна реалізація того або іншого способу захисту даних, і вміння адміністратора баз даних застосувати можливості сервера в цьому випадку відіграє немаловажну роль. Нижче приводяться деякі рекомендації із забезпечення безпеки для адміністраторів мереж і баз даних, не згадані в попередніх розділах даної статті.

5.6.1 Відключення непотрібних служб

Багато хто зі служб SQL Server відключені за замовчуванням, і при відсутності реальної необхідності їхнього застосування рекомендується залишити їх у неактивному стані. Так, підтримка застосування Microsoft.NET Framework у ядрі СУБД повинна бути включена тільки в тих випадках, коли використання керованого коду в додатку дійсно необхідно. Не рекомендується без необхідності включати такі служби й опції, як Database Mail й SQL Mail, AdHoc Remote Queries, Web Assistant, Remote DAC (Dedicated Administrator Connection), робити доступної збережену процедуру xp_cmdshell для виконання команд операційної системи з ядра СУБД і засобу застосування COM-розширень функціональності сервера (OLE Automation extended stored procedures), створювати крапки доступу по протоколі HTTP (HTTP Endpoints, рисунок 3.8).

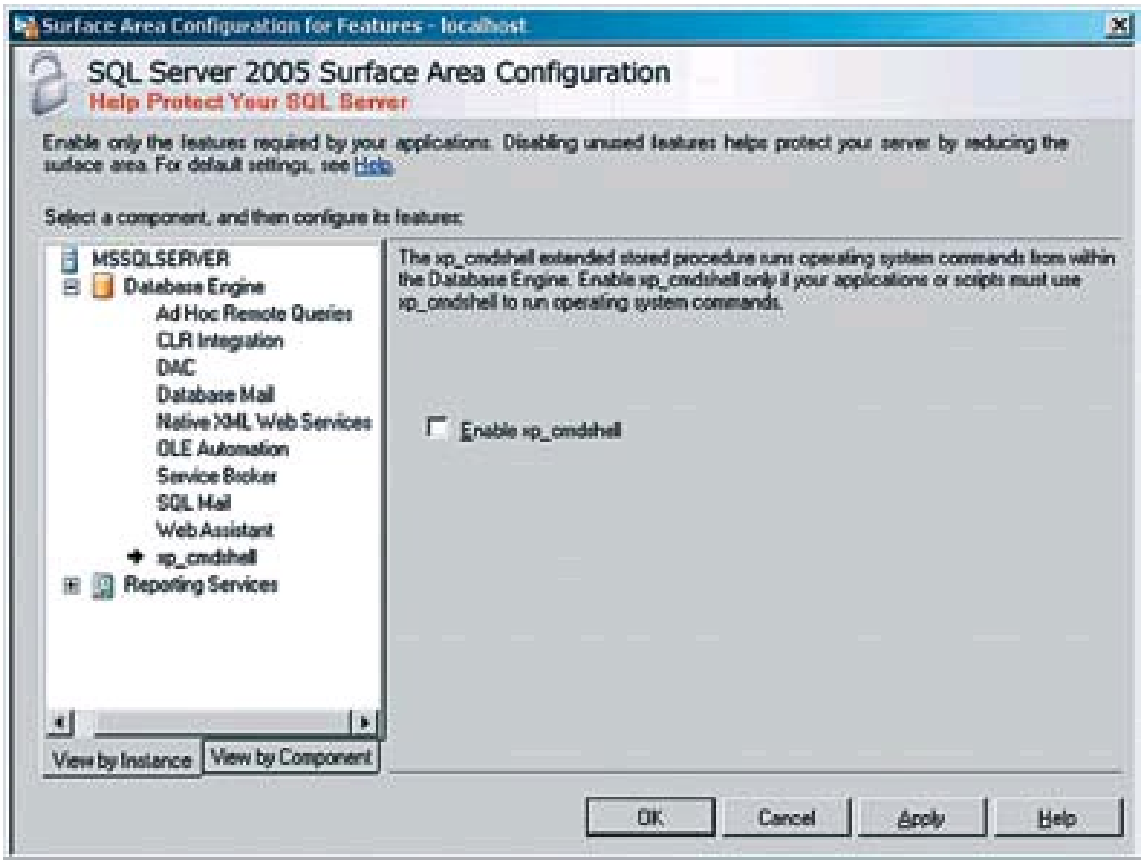

Рисунок 3.8 - Управління доступністю служб SQL Server 2005

5.6.2 Застосування брандмауера при HTTP-доступі до сервера

Оскільки атаки із застосуванням протоколу HTTP є сьогодні одним з найпоширеніших видів атак, надавати доступ до SQL Server по протоколі HTTP через Інтернет треба тільки у випадку реальної необхідності. Не варто нагадувати, що такий доступ повинен бути реалізований тільки через брандмауера.

5.6.3 Забезпечення безпеки файлів і папок

Деякі служби SQL Server (наприклад, служби повідомлень) використають ряд файлів і папок для зберігання конфігураційної інформації й даних додатків. Ядро служб повідомлень (або інших служб SQL Server) повинне мати доступ до цих файлів і папок, але користувачі не повинні мати можливості вносити зміни у файли, що втримуються в них. Для захисту файлів і папок, використовуваних службами повідомлень, можна використати дозволи NTFS для обмеження доступу до папок і файлів або механізми Encrypted File System (EFS) для шифрування файлів і папок і запобігання неавторизованого доступу (рисунок 3.9).

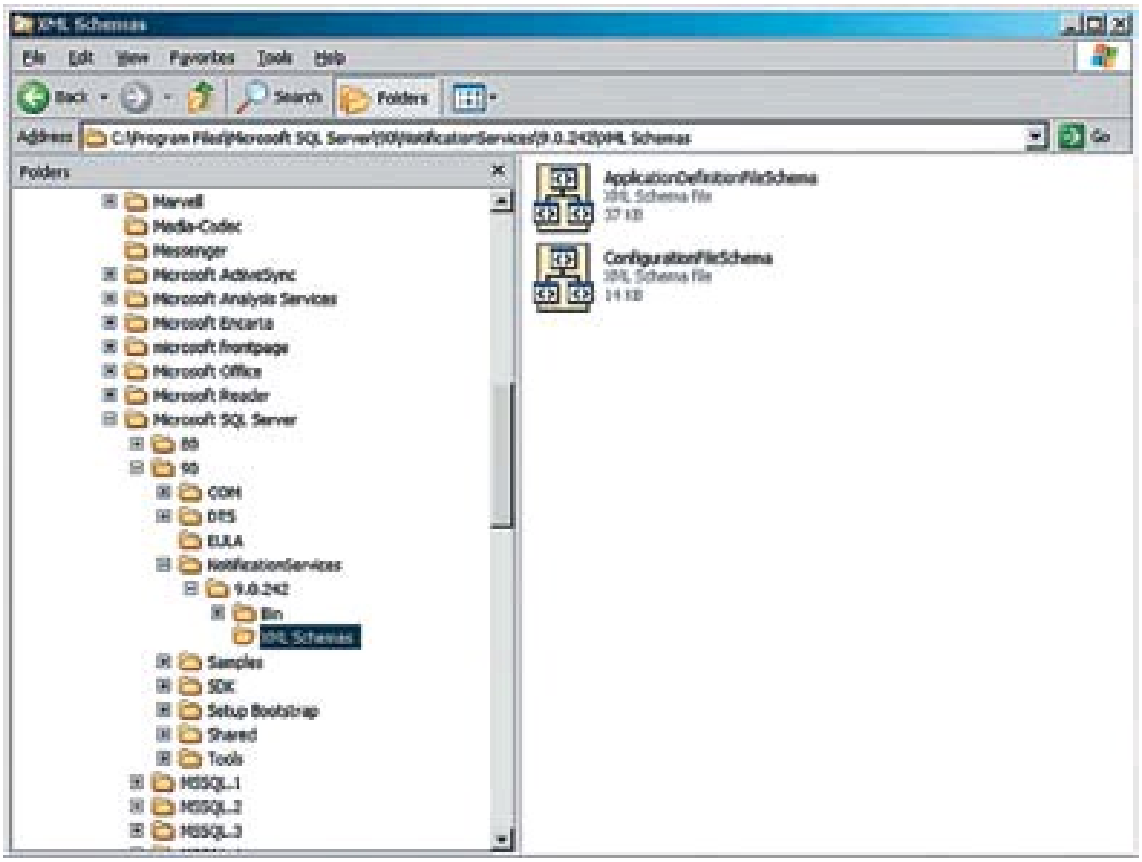

Рисунок 3.9 - Управління доступністю служб SQL Server 2005

5.6.4 Захист даних, реплікованих через Інтернет

При необхідності реплікації даних через Інтернет в SQL Server 2005 можна використати два способи захисту даних.

По-перше, можна створити канал віртуальної приватної мережі (VPN-канал) між реплікованими серверами. Цей спосіб зручний у випадку транзакційної або snapshot-реплікації.

По-друге, можна використати web-синхронізацію. Даний спосіб зручний при використанні реплікації з об'єднанням (Merge Replication), тому що в цьому випадку підтримується SSL-шифрування із застосуванням протоколу HTTPS.

5.6.5 Відновлення засобів безпеки

При створенні сучасних СУБД, так само як і багатьох інших продуктів, виробники звичайно припускають, що з появою нових погроз засобу безпеки продуктів прийде обновляти. Відновлення безпеки SQL Server знайти й установити нескладно, і якщо вибрати відповідну опцію, ці відновлення будуть завантажуватися із сайту виробника й установлюватися автоматично.

5.7 Основні рекомендації для розроблювачів додатків

Недостатня компетентність й акуратність розроблювачів додатків нерідко являє собою значно більше серйозну погрозу безпеки, ніж безвідповідальність кінцевих користувачів й адміністраторів. Саме тому ми порахували доречним нагадати кілька базових принципів, що забезпечують безпеку додатків, що застосовують СУБД:

Відмова від динамічно формованих у додатку запитів і генерації команд, виконуваних на сервері, безпосередньо з уведених користувачем даних, на користь подань, збережених процедур або параметризованих запитів.

Перевірка користувальницького уведення.

Нижче ми обговоримо ці принципи більш докладно.

5.7.1 Використання подань

Подання можна використати як механізм забезпечення безпечного доступу до об'єктів бази даних. Використання подань забезпечує простий механізм фільтрації інформації, доступної користувачам, запобігає безпосереднє звертання до таблиць, дозволяє обмежити доступ до записів, полів, метаданих залежно від завдань користувача або додатка. Крім того, використання подань дозволяє обмежити доступні користувачам операції. Так, можна вказати, що подання підтримує тільки конструкцію SELECT - у цьому випадку користувачі не можуть обновляти дані.

Використання подань дозволяє ізолювати додатка від внесення змін у схеми даних, що спрощує супровід клієнтських додатків, дозволяючи уникнути розгортання їхніх нових версій. Крім того, подання можна використати для об'єднання даних з декількох таблиць із метою обчислення агрегатних даних без надання відомостей про їхні складові. Проте не рекомендується створювати подання на основі інших подань - подібний підхід до проектування баз даних може привести до зниження продуктивності й створенню додаткового числа тимчасових таблиць.

5.7.2 Використання збережених процедур

Для виконання більшості операцій з даними додатка можуть використати або збережені процедури, або динамічно формовані в додатку запити. З погляду безпеки динамічно формовані в додатку запити володіють рядом серйозних недоліків. Так, вони дозволяють виконувати атаки типу SQL Injection (уведення

доліків. Так, вони дозволяють виконувати атаки типу SQL Injection (уведення даних, що ініціює виконання неавторизованого запиту) або здійснити неавторизований доступ до даних. Застосування збережених процедур і параметризованих запитів із цього погляду володіє рядом переваг.

Для ілюстрації поняття SQL Injection приведемо простий приклад, узятий нами із книги Майкла Ховарда й Дэвида Леблана «Захищений код» (видавництво «Російська редакція», 2003). Уявимо собі наступний код клієнтського додатка:

String sql = «select * from customer where name= ' «+ name +» '»

значення змінної name у якому вводиться користувачем. Якщо користувач увів у цю змінну значення «Іванов», він одержить записи таблиці Customer, що містять у поле Name значення «Іванов».

Але якщо він увів у це поле наступне значення:

Іванов' or 1=1 -

те така команда поверне всі рядки таблиці - запису таблиці Customer, що містять у поле Name значення «Іванов», плюс запису, що задовольняють умові 1=1 (тобто всі записи таблиці!). А якщо зловмисник увів у це поле значення

Іванов' drop table customer

- або, не дай боже, фрагмент коду з викликом збереженої процедури xp_cmdshell, що по недогляду адміністратора бази даних виявилася доступної, наслідки можуть бути самими жалюгідними.

З погляду безпеки додатки не повинні використати конструкції SELECT, INSERT, UPDATE й DELETE для запитів до бази даних. Замість цього вірніше звертатися до збережених процедур, що виконують подібні операції. Крім того, їхнє застосування дозволяє відмовитися від надання користувачам прав доступу до таблиць і подань. Відзначимо, що застосування збережених процедур дозволяє зробити клієнтські додатки незалежними від схеми бази даних, що дозволяє змінювати неї без необхідності внесення змін у сам додаток. Це спрощує супровід таких додатків, дозволяючи уникнути розгортання його нових версій.

Використання збережених процедур у ряді випадків дозволяє виконувати операції над конфіденційними даними усередині сервера, не надаючи їхньому клієнтському додатку, а також скоротити мережний трафик - при їхньому грамотному проектуванні значна частина обробки даних може бути здійснена на сервері, а не в додатку.

Втім, і збережені процедури самі по собі не є панацеєю від всіх лих. Розглянемо ще два приклади, наведених у книзі Майкла Ховарда й Дэвида Леблана. Уявимо собі наступний код клієнтського додатка, що використає збережену процедуру sp_GetName для одержання записів про конкретного клієнта:

```
Sqlstring = @» exec sp_GetName '» + name + +» '»;
SqlCommand cmd = new SqlCommand (sqlstring, sql);
```

Якщо користувач увів у поле Name

```
Іванов' or 1=1 -
```

він не одержить всі рядки таблиці. Але, увівши

```
Іванов' drop table customer -
```

він видалить таблицю, як й у попередньому випадку. І нарешті, збережені процедури бувають і такими:

```
CREATE PROCEDURE
sp_MyProc @input varchar(128)
AS exec (@input)
```

Ця процедура просто виконує уведений користувачем код і створює серйозну погрозу безпеки. Проте випадки створення настільки небезпечних процедур іноді відбуваються. Щоб уникнути подібних неприємностей, варто використати параметризовані запити й параметризовані виклики збережених процедур.

5.7.3 Перевірка користувальницького уведення

Як уникнути атак на сервер із клієнтських додатків? Для цієї мети можна скористатися вже перерахованими раніше можливостями, доступними в SQL Server 2005, такими як виконання додатків від імені облікового запису з мінімально необхідними привілеями, мінімізація привілеїв для коду, що виконує, відключення всіх непотрібних служб й опцій.

Немаловажним кроком при створенні клієнтських додатків є й перевірка даних, що вводять. Такі банальні фрагменти клієнтського коду, як перевірка відповідності типів даних, що вводять, типам у СУБД, застосування регулярних виражень у клієнтських додатках для перевірки користувальницького уведення до того, як він буде відправлений у СУБД, екранування спеціальних символів (досить часто використовуваних зловмисниками при атаках на сервери баз даних), можуть урятувати базу даних від багатьох неприємностей.

Особливо відзначимо обов'язкову при застосуванні служб повідомлень необхідність перевірки інформації, що вводить користувачами, у поля протоколу Subscriber, Subscriber Device й Subscription Information - самі служби повідомлень не містять механізмів перевірки вмісту полів заголовків протоколу.

5.8 Засоби забезпечення безпеки в SQL Server 2005 й інших СУБД

Справедливості заради відзначимо, що SQL Server не єдина гарна серверна СУБД на ринку програмного забезпечення. Надійні й прості в застосуванні СУБД масштабу підприємства випускають такі компанії, як IBM, Oracle, Sybase. Засоби забезпечення безпеки в SQL Server 2005 також не унікальні - всі перераховані вище виробники СУБД піклуються про безпеку своїх продуктів не менше, ніж корпорація Microsoft. Дане твердження ілюструється наведеною вище таблицею, у якій представлене наявність засобів забезпечення безпеки в SQL Server 2005 й у різних редакціях Oracle 10g.

Механізми безпеки	SQL Server 2005 (всі редакції)	Oracle 10g Standart Edituon	Oracle 10g Enterprise Edituon	Oracle 10g Enterprise With Abvanced Security Option
Автентифікація за допомогою Windows	+			+
Шифрування трафіка	+			+
Шифрування даних	+			+
Підтримка відкритих ключів	+			+
Підтримка Kerberos	+			+
Наявність схем, не зв’язаних з обліковими записами	+	+	+	+
Ролі	+	+	+	+
Аудит	+	+	+	+
Політики	+	+	+	+

Служби сертифікатів	+	+	+	+
Виконання коду з мінімальними привілеями	+	+	+	+

Рисунок 3.10 - Засоби забезпечення безпеки Oracle й SQL Server

Відзначимо, однак, що перераховані механізми безпеки й зручні засоби їхнього адміністрування доступні у всіх редакціях SQL Server 2005, включаючи безкоштовну редакцію Express Edition і відносно недорогі версії Workgroup Edition й Standard Edition, цілком доступні невеликим підприємствам. У той же час аналогічні механізми й утиліти Oracle 10g присутні тільки в найбільш дорогій редакції цієї СУБД.

На цьому ми закінчуємо обговорення засобів безпеки Microsoft SQL Server 2005. Хоча, як ми вже помітили, саме по собі впровадження цього продукту не захистить компанію від погроз. SQL Server 2005 надає чимало можливостей забезпечити подібний захист і спростити роботу адміністраторів і розроблювачів додатків, оскільки задовольняє всім сучасним вимогам у зазначеній області.

ЛІТЕРАТУРА

1. Бармен С. Разработка правил информационной безопасности. - М.: Издательский дом ‘‘Вильямс’’, 2002. - 208 с.

2. Богуш В.М., Довидьков О.А. Теоретичні основи захищених інформаційних технологій - К.: ДУІКТ, 2006. - 508 с.

3. Глинских А. Мировой рынок систем електронного документооборота // Информационный бюллетень Jet Info. - 2002. - № 8. – 40 с.

4. Закон України “Про електронні документи та електронний документообіг” від 22 травня 2003 р. № 851-IV.

5. Закон України “Про електронний цифровий підпис” від 22 травня 2003 р. № 852-IV.

6. Информационная Безопасность открытых систем: учебник для вузов. В 2-х томах. Том 1 – Угрозы уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: Горячая линия-Телеком, 2006 – 536 с.

7. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 26.07. 99 р. № 22.

8. Саттон Майкл Дж.Д. Корпоративный документооборот: принципы, технологии, методология внедрения. СПб.: Издательство “Азбука”, 2002. – 448 с.

9. ISO/IEC 17799: Information technology - Code of practice for Information security management, 2000.

10.http://www.directum.ru/

11.http://www.softline.kiev.ua/