УДК 004.75

**В.А. Козачок, Ю. Б. Коваленко**

# ОСОБЛИВОСТІ ПОБУДОВИ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ КОРПОРАТИВНИХ МЕРЕЖАХ

В статті розглянуто особливості побудови розподілених корпоративних мереж та надана характеристика об'єктів захисту в таких мережах.Обґрунтована необхідність створення комплексних систем захисту інформації в розподілених корпоративних мережах, в яких обробляється інформація з обмеженим доступом. Розглянуті питання забезпечення збереження інформації, що накопичується в окремих файлах і базах даних. Розкриті основні принципи захисту ресурсних та фізичних об'єктів інформаційних систем. Обґрунтовані основні положення політики безпеки інформації в інформаційно-телекомунікаційних системах. Показана необхідність використання прогресивних та перспективних технологій інформаційної безпеки.

***Ключові слова:*** Розподілена корпоративна мережа,комплексна система захисту інформації,характеристика об'єктів захисту, політика безпеки інформації.

**Постановка проблеми.**

Необхідність створення комплексних систем захисту інформації визначається законодавчими та нормативними вимогами [1, 2, 3].

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Актуальність питання полягає в особливостях, які притаманні розподіленим інформаційно-телекомунікаційним системам, а саме: велика кількість споживачів; велика різноманітність вирішуємих завдань та наявність розгалужених зв'язків.

**Аналіз останніх досліджень та публікацій.** В [1 - 3, 5] регламентовані загальні вимоги щодо необхідності створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. Основні концептуальні питання інформаційної безпеки викладені в [4], а загальні питання технічного захисту інформації в інформаційних системах в [6]. На теперішній час, нажаль, недостатньо приділяється уваги методичним питанням побудови комплексних систем захисту інформації для великих розподілених корпоративних мереж.

**Метою статті** є розгляд характеристик об'єктів захисту в складних розподілених корпоративних мережах.

**Виклад основного матеріалу.**

Розподілена інформаційно-телекомунікаційна мережа (РІТМ) — це складна розподілена в просторі мережа, що складається з безлічі зосереджених (локальних) підсистем (інформаційних вузлів), що мають програмно-апаратні засоби реалізації інформаційних технологій, і безліч засобів, що забезпечують з'єднання і взаємодію цих підсистем з метою надання територіально віддаленим користувачам широкого набору послуг зі сфери інформаційного обслуговування.

Крім того, РІТМ характеризують:

- наявність прямих, зворотних, багатоканальних і розгалужених зв'язків, а також процесів управління;
- складність, що розуміється як принципова неможливість повною мірою, без додаткових умов і обмежень, мати адекватний формалізований опис;
- безліч різноманітних складових інформаційного процесу, розподілених у просторі, що безупинно змінюють один одного в часі.

По функціонально-цільовому і прикладному призначенню існуючі РІТМ можна розділити на дві групи: загального користування і спеціального призначення.

Мережі загального користування призначені для різних сфер застосування незалежно від конкретного змісту даних, оброблюваних у РІТМ. Засоби, структура і функціональні

можливості таких інформаційних систем (ІС) виявляються однаковими для багатьох випадків застосування і забезпечують широкий діапазон послуг. Це, як правило, великі системи, що використовують в якості базових комунікаційних підмереж державні системи передачі даних. Практика використання мереж загального користуванні привела до необхідності розробки програмно-апаратних засобів, що реалізують принципи відкритості, універсальності мереж і типізації технічних рішень.

Мережі спеціального призначення призначені для рішення задач у визначеній предметній чи відомчій області.

Архітектурно територіально-розподілена система являє собою сукупність локальних обчислювальних мереж (ЛОМ) з архітектурою клієнт/сервер і індивідуальні робочі станції з правом вилученого доступу, об'єднаних базовою мережею, виділених каналів зв'язку, що комутуються.

РІТМ, у свою чергу, може бути розбита на відповідні складові елементи:

- локальна обчислювальна мережа;
- канали і засоби зв'язку (КЗ);
- вузли комутації;
- умовний кабінет керівника (або будь-яке інше приміщення, де для обробки інформації використовуються різні технічні засоби);
- робоче місце віддаленого (легального) користувача системи;
- робоче місце стороннього користувача (потенційного зловмисника);
- носії інформації (магнітні, оптичні та ін.);
- друкуюча і множувальна техніка;
- окремі персональні комп'ютери і робочі станції (термінали);
- безпосередньо користувачі (звичайні люди).

Основними особливостями РІТМ є:

- територіальна віддаленість компонентів системи друг від друга й інтенсивний обмін інформацією між ними;
- широкий спектр використовуваних інформаційних технологій;
- інтеграція даних різного призначення, що належать різним суб'єктам, у рамках єдиних баз даних і, навпаки, розміщення необхідних деяким суб'єктам даних у віддалених вузлах мережі;
- абстрагування користувачів і власників даних від фізичних структур і місця розміщення даних;
- використання режимів розподіленої обробки даних;
- участь у процесі функціонуванні ІС великої кількості користувачів і персоналу;
- одночасний доступ до ресурсів ІС великого числа користувачів (суб'єктів) різних категорій;
- високий ступінь різнорідності використовуваних засобів обчислювальної техніки і зв'язку, а також їхнього програмного забезпечення;
- відсутність спеціальної апаратної підтримки засобів захисту в більшості типів технічних засобів, широко використовуваних у ІС.

Об'єднання мереж здійснюється або через загальний вузол, або шляхом створення спеціальних каналів, що з'єднують вузли однієї мережі з вузлами іншої. Якщо мережа може бути з'єднана з іншими, то вона називається відкритою, якщо не може чи не повинна з'єднуватися, то — закритою. Закриття мережі (чи її частини) для деякої категорії користувачів є одним зі способів захисту інформаційних і обчислювальних ресурсів системи.

Відомі два основних методи розподілу інформації — комутація і селекція.

Комутація здійснюється трьома способами: комутацією каналів, повідомлень чи пакетів.

Селекція ґрунтується на обраному методі доступу взаємодіючих систем до передавального фізичного середовища зв'язку, у якій одночасно поширюється безліч сигналів, формованих декількома взаємодіючими термінальними системами.

Засоби захисту і забезпечення цілісності даних і збереження ресурсів є важливим аспектом функціонування РІТС.

Об'єкти захисту – узагальнюючий термін для усіх форм існування інформації потребуючих захисти від технічних розвідок. По своєму складу об'єкти захисту можуть бути одиничними і груповими [4].

До них відносяться:

Інформаційні об'єкти ІС – будь-яка інформація (повідомлення, відомості, файли бази даних і т.ін.) у будь-яких формах її представлення (аналогова, цифрова, віртуальна, уявна й ін.)

У поняття ресурсні (програмно-апаратні) об'єкти ІС входять усі компоненти ІС, її апаратне і програмне забезпечення, процедури, протоколи, структури, що керують і т.п. (починаючи з операційних систем і закінчуючи вимикачем жилення комп'ютера). Звідси випливає, що поняття ресурсного об'єкта визначається в загальному вигляді.

До фізичних об'єктів ІС відносяться: території, будівлі, приміщення, технічне устаткування, електронні пристрої, комп'ютерна техніка, засоби зв'язку і багато чого іншого;

Користувальницькі об'єкти ІС - це в першу чергу люди, що використовують ресурси ІС, мають доступ через термінали чи робітники ЕОМ.

Логічні об'єкти ІС — це логічні операції чи процедури, результатом виконання яких є визначений висновок чи ознака (наприклад: деяка логічна операція формує повідомлення „Небезпека" при виконанні умови збігу ряду встановлених ознак „Погроза")

Безпека на мережному рівні забезпечується між кінцевими системами, незалежно від проміжних міжмережевих комутаторів і мостів рівня даних. Якщо послуги безпеки ґрунтуються цілком на протоколах мережного рівня, це забезпечує безпеку комунікацій між кінцевими системами уздовж різнорідних мереж, що формують Інтернет (Internet).

**Захист інформаційних об'єктів.**

Розглянемо питання забезпечення збереження інформації, що накопичується в окремих файлах і базах даних.

Часто файли розмішаються на різних носіях інформації і належать користувачам ІС. Їхнє колективне використання визначає необхідність в організації окремих файлів від несанкціонованого використання, а також від фізичного руйнування. Проблема ускладнюється й у зв'язку з тим, що користувачі можуть надавати свої файли іншим користувачам. Таким чином, усі файли, що захищаються, можна умовно класифікувати як: загальні, групові, особисті.

Для забезпечення збереження файлів можуть бути використані апаратні і програмні засоби захисту, а також сукупність заходів організаційного плану, що дозволяють проводити облік. збереження і використання файлів.

Файлові сервери можуть контролювати доступ користувачів до різних частин файлової системи шляхом дозволу користувачу приєднати деяку файлову систему (чи каталог) до своєї робочої станції для використання як локального диска. Це породжує дві потенційні проблеми. Перша полягає в тому, що сервер може забезпечити захист доступу тільки на рівні каталогу, тому якщо користувачу дозволений доступ до каталогу, то він одержує доступ до усіх файлів, що міститься в цьому каталозі. Щоб мінімізувати ризик у цій ситуації, важливо відповідним чином структурувати і керувати файловою системою ЛОМ.

Системи управління базами даних (СУБД), особливо реляційні СУБД. стали домінуючим інструментом збереження великих масивів інформації. Скільки-небудь розвинуті інформаційні додатки покладаються не на файлові структури операційних систем, а на багатокористувачеві СУБД, виконані в технології клієнт/сервер. У цьому зв'язку

забезпечення інформаційної безпеки СУБД, і в першу чергу їхніх серверних компонентів, здобуває вирішальне значення для безпеки організації в цілому.

Для СУБД важливі всі три основні аспекти інформаційної безпеки — конфіденційність, цілісність і доступність. Загальна ідея захисту баз даних складається в проходженні рекомендаціям, сформульованим у [5].

Організація збереження і використання інформації в базах даних (БД) має специфічні особливості. Якщо до інформації, що міститься в БД, звертаються багато користувачів, то особливо важливо щоб елементи даних і зв'язку між ними не руйнувалися. Варто також враховувати можливість виникнення помилок і різного роду випадкових збоїв Збереження, відновлення і процедури включення даних повинні бути такими, щоб система у випадку виникнення збоїв могла відновлювати дані без утрат.

Коли розглядаються процедури захисту мережних баз даних, то дані і їхні логічні структури представляються двома способами. Окремі об'єкти даних самі можуть бути об'єктами захисту, але можуть бути організовані і структури БД (сегменти, відносини, каталоги і т.ін.).

Захист БД означає захист власне даних і їхнє контрольоване використання на робочих місцях мережі, і також захист будь-якої супутньої інформації, що витягається чи генерується з цих даних.

Функції, процедури і засоби захисту, що забезпечують захист даних на робочих станціях мережі, можна описати в такий спосіб:

1. Захист змісту даних поєднує функції, процедури і засоби захисту, що попереджають несанкціоноване розкриття конфіденційних даних і інформації з БД.

2. Засоби контролю доступу дозволяють доступ до даних тільки повноважних об'єктів у відповідності зі строго визначеними правилами й умовами.

3. Керування потоком захищених даних при передачі з одного сегмента БД в іншій забезпечує переміщення даних разом з механізмами захисту, властивим вихідним даним.

4. Запобігання можливості виявлення конфіденційних значень з даних, що містяться в регулярних чи схоластичних БД, у результаті виявлення статистично достовірної інформації.

5. Контроль погодженості при використанні БД припускає процедури захисту, що забезпечують захист і цілісність окремих елементів даних. Успішна реалізація таких процедур у ІС означає, що дані в БД завжди логічно зв'язані і значення критичних даних передаються від вузла до вузла тільки при наявності спеціальних повноважень

6. Контекстний захист даних, характерна для схем захисту динамічних БД, також повинна бути включена до складу процедур захисту БД. У цьому випадку захист окремого елемента БД у кожний момент часу залежить від проведення всієї системи захисту, а також попередніх операцій, виконаних над цим елементом (залежність від передісторії).

7. Запобігання створення несанкціонованої інформації припускає наявність засобів, які попереджають, що об'єкт одержує (генерує), інформацію, яка перевищує рівень прав доступу, і здійснює це, використовуючи логічний зв'язок між даними в БД.

Відомі два способи захисту даних у мережних базах. Перший, найбільш очевидний, полягає в забороні доступу до даних користувачів мережі, що не має права доступу до них. Керування доступом дозволяє регулювати перегляд, зміну і видалення даних і програм. Подібне керування запобігає випадковому чи навмисному виявленню, чи зміну, знищення записів і наборів даних.

Другий, також ефективний спосіб захисту баз даних у ІС, складається в забезпеченні гарантованого доступу до усіх необхідних даних тим користувачам мережі, які правильно використовують можливості і свої права.

**Захист ресурсних об'єктів.**

З кожним об'єктом ІС зв'язана деяка інформація, що однозначно ідентифікує його. Це можуть бути число, рядок символів, алгоритм, що підтверджують дійсність об'єкта. Визначимо таку інформацію як ідентифікатор об'єкта. Процес верифікації цього

ідентифікатора назвемо ідентифікацією об'єкта. Якщо об'єкт має деякий ідентифікатор зарезервований у мережі, він називається легальним об'єктом; інші об'єкти відносяться до нелегального.

Ідентифікація захищеного об'єкта — одна з функції підсистеми захисту, виконуваний у першу чергу, коли об'єкт намагається ввійти в мережу. Якщо процедура завершується успішно, об'єкт є легальним для даної мережі. Наступний крок — верифікація ідентифікатора об'єкта, що встановлює, що передбачуваний легальним об'єкт дійсно такий, яким себе повідомляє.

Після того як об'єкт ідентифікований і верифікований, повинні бути встановлені сфера його діяльності і доступні ресурси ІС. Така процедура називається наданням повноважень. Перераховані три процедури ініціалізації відносяться до єдиного об'єкта ІС, і тому їх варто віднести до засобів захисту самого об'єкта.

Основними функціями, що повинні здійснювати в цих цілях засоби захисту, є:

- ідентифікація суб'єктів і об'єкта;
- розмежування, а при необхідності і повній ізоляції доступу до обчислювальних ресурсів і інформації;
- реєстрація дій у системі.

Процедура ідентифікації і підтвердження дійсності припускає перевірку, чи є суб'єкт, що здійснює доступ до об'єкту, до якого здійснюється доступ тим, за кого себе видає. У системах, що забезпечують високу безпеку, може знадобитися періодичний повторний огляд дійсності.

У процедурі ідентифікації використовуються різні методи: прості, складні чи одноразові паролі, обмін питаннями і відповідями з адміністратором через відповідну програму, ключі, магнітні карти, значки, жетони, засоби аналізу індивідуальних характеристик (голосу, відбитків пальців, геометричних параметрів рук чи обличчя), спеціальних ідентифікаторів чи контрольних сум для апаратури, програм і даних.

Засоби реєстрації, як і засоби контролю доступу, відносяться до ефективних заходів протидії несанкціонованим діям Однак, якщо засоби контролю доступу призначені для запобігання таких дій, то задача реєстрації - знайти вже виконані дії чи їхні спроби.

Витрати, пов'язані з реалізацією розглянутих принципів, невеликі. Однак вони сприяють, як підвищенню ефективності системи, так і забезпеченню збереження.

**Захист фізичних об'єктів ІС.**

Історично склалося так, що до моменту виникнення проблеми захисту інформації засоби охорони вже існували Однак варто пам'ятати, що для захисту інформації й об'єктів, де вона зберігається, обробляється і циркулює, використовуються більш складні і досконалі засоби.

До технічних засобів охорони (ТЗО) відносять механічні, електромеханічні, оптичні, акустичні, лазерні, радіохвильові й інші пристрої, системи і спорудження, призначені для створення перешкод на шляху до інформації, що захищається, і здатні виконувати функції захисту [6].

ТЗО являють собою перший рубіж захисту інформації й елементів обчислювальних систем, а тому забезпечення фізичної цілісності таких систем і їхніх пристроїв є необхідною умовою захищеності інформації.

Перелічимо основні задачі, розв'язувані фізичними засобами ЗІ:

1. Охорона території;
2. Охорона внутрішніх приміщень і спостереження за ними;
3 Охорона устаткуванні і переміщуваних носіїв інформації;
4. Здійснення контрольованого доступу в захищені зони;
5 Нейтралізація випромінювань, і наведень;
6. Перешкода візуальному спостереженню;
7. Протипожежний захист;

8. Блокування дій зловмисника.

Захист об’єктів ІС полягає в створенні інтегрованих систем безпеки використовуваних інформаційних технологій. Майбутнє систем захисту - це централізоване керування і єдині "точки виходу" для користувачів. Сервер санкціонування чи єдиний сервер паролів містить не тільки бази даних паролів, але і правила обмеження прав і доступу. У таких централізованих системах адміністратор може керувати доступом і перевіркою повноважень з одного пункту. Таким чином, єдиний спосіб забезпечити безпеку комп’ютерних мереж — це змусити всі засоби захисту працювати, як єдине ціле.

Основними проблемами в процесі захисту інформації в ІС є:

- запобігання витоку, розкрадання, утрати, перекручування, підробки інформації;
- запобігання погроз безпеки особистості, суспільства, держави;
- запобігання несанкціонованих дій щодо знищення, модифікації, перекручування, копіювання, блокування інформації;
- запобігання інших форм незаконного втручання в інформаційні ресурси й інформаційні системи;
- забезпечення правового режиму документованої інформації як об’єкта власності;
- захист конституційних прав громадян на збереження особистої таємниці і конфіденційності персональних даних, що маються в інформаційних системах;
- збереження державної таємниці, конфіденційності документованої інформації відповідно до законодавства;
- гарантія прав суб’єктів в інформаційних процесах і при розробці, виробництві і застосуванні інформаційних систем, технологій і засобів їхнього забезпечення.

У світовій практиці вже давно використовується таке поняття, як комплексна система захисту інформації (КСЗІ), під якою мається на увазі єдина сукупність законодавчих, організаційних, програмних і технічних заходів, спрямованих на виявлення, відображення і ліквідацію різних видів погроз безпеки.

КСЗІ дозволяє:

- за допомогою центральної станції керуванні робити збір інформації з усіх пристроїв ідентифікації і контролю, обробляти її і керувати виконуючими пристроями;
- збирати й обробляти інформацію з устаткування охоронних систем сигналізації, систем відео спостереження, пожежогасіння, вентиляції, енергопостачання й ін.;
- створювати журнали обліку стану цих систем і змін, що відбуваються, демонструвати оператору стан систем і аварійні ситуації в текстовому чи графічному виді;
- при підключенні інформаційних каналів, що зв’язують головний об’єкт з філіями чи іншими об’єктами, центральний оператор одержує можливість контролювати стан усієї структури в реальному режимі часу.

Однак, найчастіше, необхідність комплексного забезпечення безпеки організації не знаходить належного розуміння в користувачів. В даний час більшість організацій намагаються вирішувати питання створення систем безпеки власними силами.

Такий підхід приводить до наступних негативних наслідків:

- створення ефективно діючої системи безпеки розтягується на великий термін;
- деякі організації не мають свою внутрішню службу безпеки чи хоча б співробітника, що грамотно змогли б вирішити всі питання безпеки;
- керівники організацій, самі навіть усвідомлюючи, що повинні бути надійні системи безпеки, не можуть перебороти бар'єр необхідності установки цих систем у себе в організації. В одних цей бар'єр виражається в недостачі коштів, а інші не зважуються на придбання й установку систем безпеки, поки самі не переконаються в можливості несанкціонованого доступу до їхньої інформації;
- використання тільки тих технічних і технологічних рішень, що відомі співробітникам служб безпеки організації, приводить до застосування застарілих методів і засобів захисту, що у свою чергу може стати реальною погрозою для ІС.

**Висновок.**Для того, щоб забезпечити надійний захист ресурсів корпоративних інформаційних систем на сьогодні і на найближче майбутнє, у системі інформаційної безпеки повинні бути реалізовані самі **прогресивні й перспективні технології інформаційної безпеки**. До них відносяться:

- комплексний підхід до формування інформаційної безпеки, що забезпечує раціональне об'єднання технологій ізасобів інформаційного захисту;
- застосування захищених віртуальних мереж VPN для захисту інформації, переданої по відкритих каналахзв'язку;
- криптографічне перетворення даних для забезпечення цілісності, дійсності й конфіденційності інформації;
- застосування міжмережевих екранів для захисту корпоративної мережі від зовнішніх погроз при підключенні до загальнодоступних мереж зв'язку;
- керування доступом на рівні користувачів і захист від несанкціонованого доступу до інформації;
- гарантована ідентифікація користувачів шляхом застосування токенів (смарт-карт, touch-memory, ключів для USB-портів і т. ін.) і інших засобів аутентифікації;
- підтримка інфраструктури керування відкритими ключами;
- захист інформації на файловому рівні (шляхом шифрування файлів і каталогів) для забезпечення її надійногозберігання;
- захист від вірусів з використанням спеціалізованих комплексів антивірусної профілактики й захисту;
- технологія виявлення вторгнень (Intrusion Detection) і активного дослідження захищеності інформаційних ресурсів;
- централізоване керування засобами інформаційної безпеки.

Наявність централізованих засобів керування продуктами безпеки є обов'язковою вимогою для можливості їхнього застосування в корпоративному масштабі.

Подальші дослідження доцільно зосередити на розробку методичного апарату створення комплексних систем захисту інформації для розподілених інформаційно-телекомунікаційних мереж.

**Література**

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 5 липня 1994 року № 80/94-ВР, Відомості Верховної Ради України (ВВР), 1994, № 31, - с.286.

2. Постанова КМ України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" № 373 від 29 березня 2006 року. [Електрон. ресурс]: - Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=47960&cat_id=38834.

3. НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі". [Електрон. ресурс]: - Режим доступу:http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=46074&cat_id=38835.

4. Методика информационной безопасности. / [Уфимцев Ю.С., Буянов В.П., Ерофеев Е.А и др.] – М.: Издательство "Экзамен", 2004. – 544 с.

5. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу". [Електрон. ресурс]: - Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40386&cat_id=38835.

6. Торокин А.А. Основы инженерно-технической защиты информации. – М.: изд-во "Ось-89", 1998. – 336 с.

Надійшла 19.02.2015 р. Рецензент: д.т.н., проф. Шелест М.Є.