УДК 681.322

ЗАСТОСУВАННЯ ПРОГРАМНИХ ЗАСОБІВ РОЗМЕЖУВАННЯ ДОСТУПУ ДО ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ ДОВІДКОВО-РОЗРАХУНКОВИХ СИСТЕМАХ ВІЙСЬК ППО

к.т.н. С.І. Карпов, к.т.н. Л.І. Матюшенко, к.т.н. С.Г. Назаренко
(подав д.т.н. Г.В. Пєвцов)

Розглянуто вимоги до засобів розмежування доступу до інформації в інформаційних довідково-розрахункових системах (ІДРС) військ ППО. Обґрунтовано вибір засобу розмежування доступу до інформації у ІДРС. Запропоновано концептуальну модель розмежування доступу до записів таблиць баз даних.

Постановка проблеми. Функціонування ІДРС Військ ППО Збройних Сил України (ЗСУ) характеризується такими чинниками:

– багатокористувацьким доступом до інформації і режимів роботи системи. Робота конкретної ІДРС апріорно припускає існування різних користувачів з різними правами доступу до ієрархічно структурованої інформації. Наприклад, начальнику штабу зенітної ракетної бригади (зрбр) повинна бути надана повна інформація тільки про його зрбр, начальнику зв'язку бригади – тільки для вирішення задач забезпечення зв'язку, а начальнику Головного штабу Військ ППО ЗСУ – повна інформація за всіма з'єднаннями;

– різноманітністю рівнів таємності інформації;

– існуванням багатьох інформаційно взаємодіючих між собою локальних мереж. Наприклад, частина інформації, введеної в зрбр, використовується для окремих потреб бригади, інша передається у вищу локальну мережу для використання (інформація про чергові сили бригади, розміщення зенітно-ракетних комплексів (ЗРК) та ін.). В зв'язку з цим необхідно забезпечити цілість інформації на рівні передачі в глобальній мережі;

– актуальністю і важливістю, які визначають порядок передачі інформації між взаємодіючими локальними мережами.

Під правом доступу до інформації розуміємо дозвіл на отримання доступу до деякого об'єкта в БД та інтерфейсу програмного комплексу (таблиць, переглядів, збережених процедур та ін.). Права надаються деякому запису користувача або ролі й дозволяють їм виконувати певні операції.

Таким чином, задача розмежування доступу до інформації, що циркулює в ІДРС військ ППО, з боку різних посадових осіб командних пун-

ктів та штабів є однією із актуальних при створенні таких систем.

Аналіз літератури. Серед засобів розмежування доступу традиційно виділяють [1 – 3]:

– ***організаційні заходи*** розмежування доступу до інформації, що полягають в розробці правил користування технічними і програмними засобами, розмежуванні фізичного доступу до каналів зв'язку і технічних засобів, створенні рівнів таємності тощо. Дуже часто при проектуванні системи захисту з уваги випускається найважливіша ланка – фізичний захист самого сервера. Якщо сервер можна перемістити з його законного місця, то засоби злому або знищення інформації завжди можна знайти. Це відноситься і до серверних носіїв: стрічкових приладів і дискової пам'яті. При створенні локальної мережі неприпустимою є наявність неконтрольованих мережних розломів;

– ***технічні засоби*** розмежування доступу до інформації, що призначені для ідентифікування користувачів для роботи на об'єктах, які містять інформацію. Для підвищення загального рівня захищеності мережного середовища необхідно забезпечити усіх користувачів платами SecureID або їм подібними. Ці прилади генерують постійно змінні паролі, аутентифікація яких виконується мережним файл-сервером. В цьому випадку користувачі без врахованих ідентифікаційних плат не зможуть отримати доступ до локальної мережі, навіть підключившись до мережного роз'єму;

– ***програмні засоби*** розмежування доступу до інформації, що призначені для реєстрації користувачів в інформаційній системі і визначення можливостей користувачів при роботі з прикладним забезпеченням (ПЗ).

Серед програмних засобів розмежування доступу можна виділити такі засоби: загального програмного забезпечення, СУБД, програмного комплексу.

При розробці програмних засобів розмежування доступу необхідно органічно використовувати існуючі програмні засоби і знов створені. При розмежуванні доступу до інформації можна виділити два основних напрямки розмежування: ***розмежування до дій*** (врахування цього напрямку при розробці програмних засобів захисту необхідне для контролю доступу до функціональності програмного комплексу; цей напрямок може бути реалізований тільки всередині програмного комплексу ІДРС); ***розмежування до інформації*** (цей напрямок враховує розмежування доступу як до стовпчиків, так і до рядків інформації, яка в реляційних СУБД подана у вигляді таблиць; ієрархічне подання інформації, що використовується в ІДРС, також активно застосовується в алгоритмах розподілу доступу; цей напрямок може бути реалізований і всередині програмного комплексу ІДРС, і засобами СУБД).

Мета статті: розробка пропозиції щодо засобу розмежування доступу до інформації в ІДРС військ ППО та розробка алгоритму розмежу-

вання доступу до записів таблиць бази даних.

Основний розділ. ІДРС військ ППО функціонує в середовищі Windows NT з використанням СУБД MS SQL Server, тому був обраний стандартний засіб захисту, який передбачає комбінацію засобів захисту SQL Server і Windows NT. Цей засіб визначає, як користувачі будуть реєструватися на сервері і яким чином вони будуть входити в систему Windows NT. При встановленні SQL Server в системі автоматично визначаються два облікових записи. Перший – це системний адміністратор під іменем SA. Другий представляє користувача під іменем Guest і забезпечує дозволений за умовчуванням рівень доступу до системи. Обліковий запис SA є особливим записом і забезпечує повний контроль над різними аспектами роботи системи. Тому винятково важливо замінити порожнє значення паролю, що апріорно присвоюється йому, іншим, який забезпечує більший рівень захисту. В стандартному режимі система здійснює повний контроль і управління обліковими записами, призначеними для доступу до сервера. SQL Server працює з двома рівнями доступу користувачів. Перший рівень – це облікові записи. Обліковий запис призначений для підключення безпосередньо до сервера системи SQL Server. Область дії облікового запису розповсюджується на весь сервер (тобто на всі бази даних (БД)). Всі облікові записи зберігаються в таблиці sysxlogins основної БД сервера master. Запис користувача – це засіб, який обраний в SQL Server для контролю за тим, хто має права на доступ до певних ресурсів сервера. Під ресурсами маються на увазі таблиці, перегляди і збережені процедури БД сервера. Всі записи користувачів зберігаються в таблиці sysusers, яка існує в кожній БД.

SQL Server підтримує можливість створення і використання ролей, що дозволяє надавати однакові права доступу всім, кому ця роль призначається. Подібний підхід істотно спрощує організацію захисту. Будь-якому користувачеві можна призначити стільки ролей, скільки необхідно. Це правило дозволяє зв'язати облікові записи користувачів з набором прав доступу, що йому надаються. Крім того, слід враховувати, що область дії ролі розповсюджується тільки на певну базу даних. Це означає, що якщо деяка роль визначена тільки в одній БД, то в усіх інших вона буде недосяжна. При необхідності можна визначити відповідну роль в кожній з БД окремо. Для спрощення цієї процедури можна використати БД model (використовується як шаблон для знов створюваних БД).

Серед операцій доступу до деякого об’єкта в БД виділимо такі: вибору даних з таблиць або переглядів; запису нових даних в таблиці або перегляди; зміни існуючих даних в таблицях або переглядах; видалення даних з таблиць або переглядів; виконання збережених процедур.

Всі права доступу автоматично надаються володарю або створювачу об'єкта. В подальшому володар може прийняти рішення про надання ін-

шим користувачам або їхнім групам прав, які їм потрібні.

В SQL Server для призначення і відміни прав доступу використовуються команди GRANT і REVOKE. Синтаксис команди GRANT наведено на рис. 1, а; приклад використання для надання прав доступу до таблиці «Організаційна структура» – на рис. 1, б.

```
GRANT перелік_прав
ON ім'я_об'єкта
TO список користувачів
```

а)

```
GRANT SELECT, UPDATE, DELETE
ON OrganizationScheme
TO public
```

б)

Рис. 1. Команда GRANT

Одним з програмних засобів розмежування доступу в SQL Server є перегляди, оскільки вони обмежують доступ користувачів до даних за своїм призначенням. Наприклад, для користувачів n-го корпусу ППО можна створити перегляд, що містить обмеження на дані тільки n-го корпусу. Дані програмні засоби при розробці ІДРС були застосовані для розмежування доступу службових осіб до інформаційних стовпчиків. Для розмежування доступу до записів таблиць БД ІДРС розроблено концептуальну модель (рис. 2).

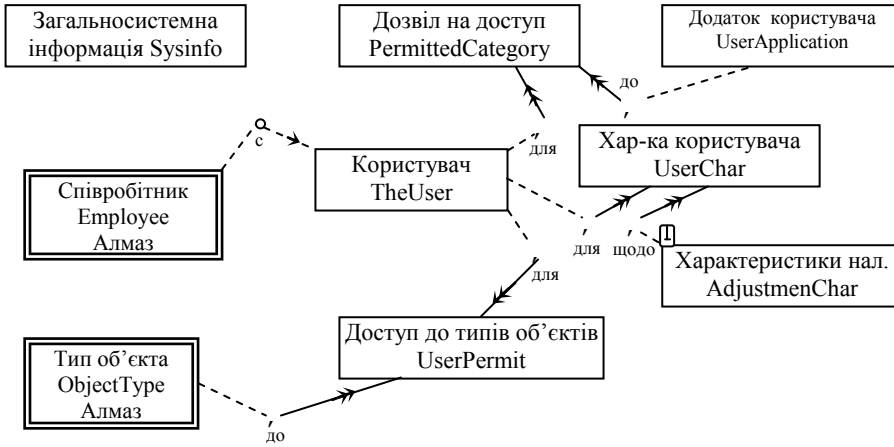

Рис. 2. Концептуальна модель "Разграничение доступа"

Новим є наступне. В підмоделі «Системна інформація» додано сутність «Доступ до типів об'єктів», що служить для зберігання інформації про доступ кожного користувача до типів об'єктів і організаційної структури ІДРС (сутність «Тип об'єкта», «Організаційна структура»). Під категорією доступу розуміється *повний доступ*, якій надає можливість перегляду, додавання, зміни і видалення інформації, або *обмежений доступ*, якій дозволяє використовувати інформацію тільки для перегляду. Адміні-

стратор БД, використовуючи програму адміністрування, призначає користувачам категорію доступу до типів об'єктів і організаційних структур. Так, для ролі користувача «Командир зрбр» призначається повний доступ до типу об'єкта «m-та зрбр» і всіх підпорядкованих об'єктів: полків, дивізіонів тощо. Для користувача «Командир m-ої зрбр» встановимо повний доступ до організаційної структури «m-та зрбр». Через те, що m-та зрбр має декілька підпорядкованих об'єктів (особовий склад, озброєння, дислокація тощо), то даному користувачеві буде відкрито повний доступ і для цих об'єктів. Також розроблено службові збережені процедури для організації розмежування доступу з використанням методики переглядів. Наведемо перелік даних процедур і їхнє призначення: *sp_IsGrantObject* призначена для перевірки наявності повного доступу до означеного типу об'єкта; *sp_AddDropLogin* призначена для вставлення нового облікового запису і нового запису користувача; *sp_GetOTViewName* визначає префікс для створення переглядів доступу до об'єктів за поточним кодом користувача (@UserID); *sp_InstallViewObjectType* служить для створення перегляду для доступу користувача. Перегляд формується на підставі даних з таблиці "Доступ до типів об'єктів"; *sp_InstallAllViewObjectType* створює перегляди доступу для всіх користувачів системи; *sp_AddPermitToSubordination, sp_DeletePermitToSubordinatio*, *sp_DeleteViewObjectType*, *sp_RevokeOT* служать для управління правами доступу користувачів і взаємодії з механізмами захисту MS SQL Server.

Висновок. Обраний засіб розмежування доступу до інформації, якій є комбінацією засобів захисту SQL Server і Windows NT, дозволяє задовольнити вимогам, що пред'являються до розмежування доступу до інформації в ІДРС військ ППО, та може бути використаний при створенні перспективних ІДРС.

ЛІТЕРАТУРА

1. *Кен Хендерсон. Delphi-3 системы клиент-сервер. Руководство разработчика. – К.-М.: Питер, 1998. – С. 391 – 411.*
2. *Адам Деннинг. Active X для профессионалов. – С.-Пб.: Питер, 1998. – С. 46 – 91.*
3. *Данылив И.В., Лукашин С.О., Назаренко С.Г. Движущие силы развития CASE-средств // Корпоративные системы. – 2002. – № 1. – С. 31 – 35.*

Надійшла 15.09.2003

***КАРПОВ Сергій Іванович**, канд. техн. наук, снс НДЛ Харківського військового університету. Закінчив ХВУ в 1995р. Область наукових інтересів – бази даних.*

***МАТЮШЕНКО Леонід Іванович**, канд. техн. наук, заст. начальника науково-дослідного управління наукового центру при ХВУ. Закінчив КВІРТУ ППО в 1983р. Область наукових інтересів – автоматизовані системи управління і обробки інформації.*

НАЗАРЕНКО Сергій Геннадійович, *канд. техн. наук, заст. начальника НДВ наукового центру при ХВУ. Закінчив ХВВКІУ РВ в 1992 р. Область наукових інтересів – бази даних.*