УДК 004

В. Б. Дудикевич, Б. М. Березюк, А. З. Піскозуб
Національний університет "Львівська політехніка",
кафедра захисту інформації

ОСОБЛИВОСТІ БУДОВИ ТА ЗАХИСТУ КОРПОРАТИВНИХ СХОВИЩ ДАНИХ

Розглянуто особливості будови сховищ даних та проаналізовано найпоширеніші види систем зберігання даних. Сформульовано базові задачі комплексного захисту корпоративного сховища даних та розглянуто програмно-апаратні засоби їх вирішення.

Ключові слова: сховище даних, агреговані дані, захист інформації, права доступу, проксі-сервер, брандмауер, моніторинг подій, резервне копіювання, ISO 27001.

There have been considered the features of the structure of the data warehouse and analysis of the most common types of storage systems. There have been formulated the basic tasks of comprehensive protection of corporate data storage and reviewed software and hardware to solve them.

Key words: data ware house, aggregate data, information security, permissions, proxy, firewall, monitoring events, backup, ISO 27001.

Вступ

Сховище даних (Data Warehouse, DW) – це особливий тип бази даних, яка містить отриману з різних джерел агреговану тематичну інформацію, призначену для використання у системах аналізу та прийняття рішень. На відміну від бази даних, сховище накопичує всю необхідну інформацію для виконання задач довгострокового прийняття рішень та стратегічного керування. Інформація, яка знаходиться в сховищах даних, дає змогу, до прикладу, на основі аналізу протікання процесу протягом декількох попередніх років розробити перспективний план розвитку корпорації, окремих галузей економіки держави, банківської системи, фонду соціального страхування, надходження в бюджет податкових коштів тощо.

Інформація сховищ даних має здебільшого конфіденційний характер і її розкриття може призвести до серйозних для корпорації втрат. Тому політика безпеки мережі повинна забезпечити створення навколо DW такого периметра інформаційного захисту, який відповідав би вимогам довготривалого, надійного і захищеного зберігання.

Метою роботи є аналіз особливостей будови сховищ даних та вироблення рекомендацій з їх захисту від несанкціонованого доступу з боку як зовнішнього середовища, так і внутрішніх клієнтів, а також загроз викрадення та цілісності даних.

Особливості будови сховища даних

Сховища даних характеризуються предметною орієнтацією, інтегрованістю, мінімальною надлишковістю і незмінністю. Дані сховищ організовані відповідно до основних напрямів діяльності корпорації з урахуванням часу їх надходження. Первинні дані, які надходять у DW з оперативних баз даних, систематизуються та зводяться до єдиного формату. Вони фільтруються від надлишкових даних та таких, які не будуть використовувати системи прийняття рішень. Завантажені у сховище дані не підлягають змінам – їх можна лише зчитувати з подальшим опрацюванням.

Сховище даних функціонує у складі структури центру обробки даних і будується на базі клієнт-серверної архітектури, додатків прийняття рішень та систем управління базами даних.

Серверна частина містить сховище агрегованих даних, сховище метаданих та вітрини (кіоски) даних. Сховище агрегованих даних містить агреговану тематичну інформацію, призначену для використаннях у системах аналізу та прийняття рішень. Сховище метаданих містить інформацію про джерела, час надходження та періодичність оновлення даних, їх структуру, способи агрегації (визначення сумарних показників) та інші характеристики агрегованих даних. Кіоски даних описують конкретний вид діяльності корпорації, її філіалу або окремого підрозділу [1].

Дані у сховищі представлені у зручній для багатовимірного аналізу формі, яка дає змогу оптимізувати доступ до комірок та забезпечує швидкий пошук і вибірку потрібних даних. У спеціалізованих сховищах, основаних на багатовимірній структурі даних, дані можуть бути організовані у вигляді багатопроменевої зірки, гіперкуба або полікуба. У гіперкубах всі змінні зберігаються в комірках однакової розмірності, а в полікубах кожна змінна зберігається з власним набором вимірів. Така форма представлення даних забезпечує можливість включення в інформаційну модель різноманітних вбудованих функцій.

Сховища даних можуть бути побудовані як за відкритою структурою на базі виділених серверів з великим обсягом дискової пам'яті, так і за закритою структурою з вбудованою ОС. У сховищах можуть використовуватися різні види систем зберігання даних (СЗД), які відрізняються між собою архітектурою і способом з'єднання з клієнтською частиною мережі.

Для зберігання даних у сховищах найчастіше використовують три види СЗД:

– DAS (Direct Attached Storage), коли кошик з жорсткими дисками під'єднується безпосередньо до сервера мережі через волоконно-оптичний або мідний кабель інтерфейса Fibre Channel;

– NAS (Network Attached Storage), коли до інтерфейсу локальної мережі під'єднується спеціалізований файловий сервер з набором жорстких дисків, вбудованою ОС та набором функцій швидкого доступу до файлів;

– SAN (Storage Area Network), коли різні типи пристроїв зберігання даних (дискові масиви, бібліотеки на магнітних стрічках, DVD-диски тощо) під'єднуються до серверів через спеціальну мережу SAN на базі комутаторів. Мережа SAN забезпечує доступ будь-якого сервера локальної мереж до будь-якого пристрою зберігання даних (ПЗД).

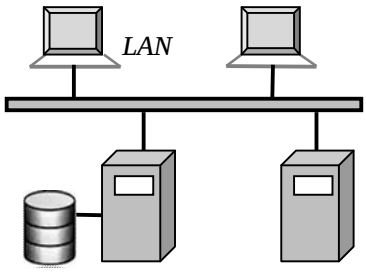

Рис. 1. Використання системи DAS

Системи DAS знайшли широке використання в корпоративних мережах завдяки простоті адміністрування та низькій вартості. DAS-система може використовувати декілька файлових серверів з індивідуально під'єднаними пристроями зберігання даних (рис. 1). Проте при виході з ладу сервера, до якого під'єднаний пристрій зберігання даних, дані стають недоступними. В сховищах невеликих офісів можуть використовувати файлові сервери з внутрішнім дисковим простором.

Системи NAS використовують, здебільшого, в мережах сімейства Ethernet. Вони забезпечують доступ великого числа як серверів, так і клієнтів локальної мережі до файлів, які зберігаються на дисках NAS (рис. 2). Проте файлові сервери системи NAS не дають змоги забезпечити швидкісний і гнучкий доступ до даних на рівні блоків, властивих системам SAN.

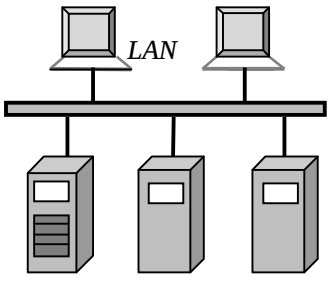

Рис. 2. Використання системи NAS

Система SAN забезпечує можливість доступу серверів сховища до будь-яких блоків даних, що містяться на зовнішніх пристроях збереження даних, з їх подальшим опрацюванням файловими серверами мережі (рис. 3). Перенесення інтенсивного трафіку записування/читання в окрему SAN-мережу дає змогу розвантажити локальну мережу та підвищити безпеку зберігання даних. Висока швидкодія та низька латентність, масштабованість і гнучкість логічної структури забезпечують системам SAN все більшу популярність.

На клієнтській стороні мережі встановлено програмно-апаратні засоби великого числа тісно пов'язаних з сховищем прикладних та обслуговуючих систем. Це прикладні системи, які, власне, і формують дані сховища, програмне забезпечення аналізу та прийняття рішень, набір програм імпорту/експорту даних, системи обробки типу ETL (extraction, transformation, loading), засоби адміністрування, моніторингу подій, копіювання даних тощо.

Робота з обслуговування сховищ даних полягає в опрацюванні даних згідно з поставленим завданням, резервному копіюванні та архівації баз даних, управлінні правами користувачів тощо. Може використовуватися гнучке конфігурування системи, коли зв'язок між клієнтською і серверною частинами здійснюється за допомогою віддалених процедур. Розробники прикладних програмних засобів можуть використовувати різні технології роботи як з локальними, так і з віддаленими базами даних. Серверна частина сховища може бути встановлена також на обладнанні провайдера або організована у вигляді розподілених хмарних систем у мережі Інтернет. Це насамперед залежить від рівня конфіденційності даних, специфіки діяльності корпорації та відсутності заборони зі сторони відповідних нормативних актів. Необхідними умовами розміщення сховища поза територією корпорації є забезпечення належного захисту даних та фінансова доцільність.

Вимоги до організації комплексного захисту корпоративного сховища даних

Об'єм даних сховища може сягати десятків *Тбайт*, а його створення може тривати декілька років. Це диктує відповідні вимоги до мережевої інфраструктури і систем зберігання та обробки інформації. Сховища даних містять, здебільшого, конфіденційну інформацію, втрата якої може призвести до значних для корпорації втрат. Тому політика безпеки мережі повинна забезпечити створення навколо DW такого периметра захисту, який відповідав би вимогам довготривалого, надійного і захищеного зберігання класу С2, а для особливо важливих та конфіденційних даних – класу В1 за класифікацією Помаранчевої книги МО США. Це стосується, насамперед, конфіденційної інформації, яка може бути пов'язаною з персональними даними, бути державною таємницею тощо.

Слід зазначити, що надійний захист сховища даних, який відповідав би вимогам вказаних класів, може бути реалізований лише у випадку створення комплексного захисту з використанням різноманітних програмно-апаратних засобів та організаційних заходів, описи та рекомендації з використання яких подані у багатьох відомих документах, зокрема ISO/SES 27001:2005 [2]. При цьому організаційні заходи передбачають обмеження фізичного доступу в приміщення центру обробки даних (організація пропускної системи, відеоспостереження, автентифікація доступу в приміщення тощо), організацію надійного збереження резервних та архівних копій даних на магнітних носіях інформації тощо.

Політика корпоративної безпеки повинна передбачити застосування багаторівневого незалежного від адміністраторів аудиту подій, що відбуваються на всіх рівнях [3]. Комплексний захист сховища даних вимагає якісного вирішення таких базових задач:

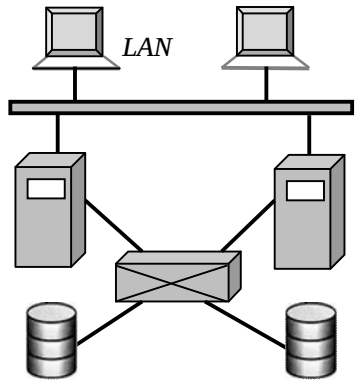

Рис. 3. Використання системи SAN

1. Захист корпоративної локальної мережі і серверів сховища від зовнішнього втручання за допомогою багаторівневого мережевого екрана з використанням проксі-функцій та NAT-механізму;
2. Використання VLAN у внутрішній локальній мережі або шифрування як даних, так і керуючих пакетів;
3. Захист інформації в процесі її передавання відкритими каналами зв'язку з використанням захищених каналів та віртуальних приватних мереж (VPN);
4. Використання багаторівневої системи захисту від вірусів і спаму, яка охоплює всі комп'ютери внутрішньої локальної мережі;
5. Аналіз мережевого трафіку з використанням програмно-апаратних засобів моніторингу мережі, в т.ч. мережевих моніторів, систем запобігання вторгнень (IDS/IPS), журналів реєстрації та ін.;

6. Виконання згідно з вимогами політики мережевої безпеки резервного копіювання та архівування зашифрованих даних сховища.

У корпоративних мережах із сховищами даних доволі ефективним є використання разом з мережевим екраном зовнішнього периметра виділеного проксі-сервера, який виконує роль посередника між серверами системи збереження даних і клієнтською частиною мережі. На рис. 4 наведено структуру LAN з використанням NAS-системи зберігання даних із вбудованою ОС, набором функцій швидкого доступу до файлів та можливістю повного дублювання головного сховища даних. Мережевий екран, побудований на базі сервера SG, виконує функції шлюзу у публічну мережу та захищає корпоративну мережу від спроб несанкціонованого проникнення пакетів з віддалених мереж, в т.ч. з мережі Internet. Розміщений у внутрішній мережі проксі-сервер PS виконує функції посередника між клієнтами і NAS-серверами сховища. Програмне забезпечення клієнтів локальної інтранет-мережі налаштоване таким чином, що всі їх запити поступають на сервер PS, який на основі заданих адміністратором правил виконує аналіз отриманих пакетів та захищає серверну частину сховища від можливих атак. Правила враховують права доступу клієнтів до системи збереження даних, критерії фільтрації пакетів тощо. У таблиці дозволів рекомендується максимально обмежити діапазони дозволених IP-адрес.

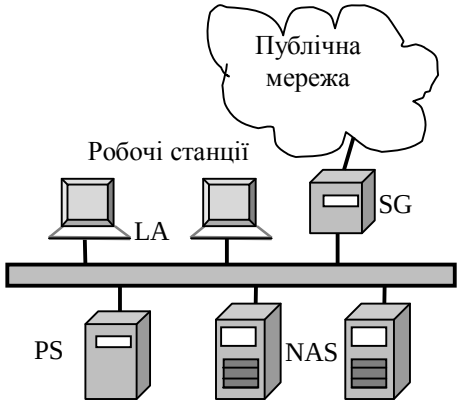

Рис. 4. Використання проксі-сервера у внутрішній локальній мережі

Якщо запит відноситься до серверів зовнішньої мережі і клієнту надано на це відповідне право, то сервер PS направляє його пакети на мережевий екран на базі SG. Сервер SG після опрацювання пакета направляє його у публічну мережу від свого імені, використовуючи тунельний режим протоколу IPSec.

Спеціальні програми антивірусного захисту сховища дають змогу виявляти і діагностувати вірусне зараження баз даних з подальшим лікуванням заражених файлів. Антивірусна програма забезпечує перевірку файлів сховища при звертанні до них з робочих станцій. Сервер PS дає змогу читати або змінювати файли, якщо антивірусна програма визнала їх безпечними. За замовчуванням спеціальна програма лікує заражені файли, а якщо лікування неможливе, то видаляє їх. Умовно заражені файли поміщаються на карантин. Перед лікуванням або видаленням файла його копія пересилається у резервне сховище. Перевірку сховища на вимогу адміністратор може запланувати заздалегідь, призначивши її на період низької активності сервера. Протоколи перевірки сховищ даних заносяться у журнал звітності.

Структуризацію внутрішньої локальної мережі та її розбиття на VLAN й шифрування внутрішніх пакетів (протоколи TLS, IPSec, SSL та ін.) виконують тоді, якщо це передбачено корпоративною політикою безпеки. При цьому через великі обсяги оброблюваної інформації шифрування даних на рівні ядра зазвичай не використовують у зв'язку з виникненням проблем з продуктивністю мережі. Для багаторівневого захисту клієнтської мережі від спаму і вірусів часто використовують систему Microsoft Fore Front, яка зарекомендувала себе як надійна і гнучка система захисту.

Контроль доступу до серверної частини сховища висуває вимоги до авторизації та багатофакторної автентифікації користувачів як на рівні операційних і прикладних систем, так і на рівні доступу до операцій з базами даних. Рівень доступу уповноваженим особам як в закриті приміщення центру обробки даних, так і до програмно-апаратних засобів та даних повинен визначатися тільки тим способом і за допомогою тих засобів, які дозволені політикою безпеки. Ця вимога стосується і механізмів контролю запуску авторизованих програм авторизованими користувачами. Використання відповідних прикладних програмних засобів і організаційних заходів дає змогу розподілити права не тільки для користувачів, але й для системного адміністратора, адміністратора баз даних та фахівців з інформаційної безпеки.

Мандатний спосіб доступу до баз даних, коли всі користувачі діляться на групи відповідно до рівня їх уповноважень та за приналежністю до тієї чи іншої групи суб'єктів, забезпечується засобами СУБД. Це дає змогу зберігати в одному сховищі даних інформацію з різним ступенем конфіденційності, обмежуючи при цьому доступ користувачів до даних відповідно до категорій їх допуску.

Для централізованого моніторингу подій у режимі реального часу доцільно використовувати *системи управління інформацією та повідомленнями безпеки* (Security Information and Event Management, SIEM) [4]. SIEM-системи забезпечують уповноважений персонал та користувачів мережі інформацією про її стан та дозволяють, відповідно до заданих правил та налаштувань, оперативно реагувати на виникнення загрозливих ситуацій. Для аудиту подій у прикладних і операційних системах та комунікаціях часто використовують системи моніторингу корпорацій Cisco Systems, CA Security Command Center, IBM Qradar та ін. Система MS SCOM (Microsoft System Center Operation Manager) забезпечує повний контроль внутрішнього стану серверів, мережі, процесів і т. п.

Менеджмент на рівні баз даних виконують засобами СУБД. Так, система SQL Server, яку використовують у сховищах технологій класу OLAP, управляє мандатним доступом до даних з врахуванням повноважень груп користувачів, забезпечує двовузлову відмовостійку кластеризацію, автоматизує передавання журналу транзакцій та формування звітів тощо.

Незважаючи на те, що в DW необхідно забезпечувати наскрізну безпеку, вирішальне значення має здатність забезпечити в сховищі даних гнучку багатошарову модель безпеки. Отже, вихід з ладу одного механізму безпеки не призводить до компрометації критично важливої інформації. Зокрема, Oracle Database 10g [Oracle whitepaper] пропонує такі рішення [5]:

- Рольове управління доступом до даних DW (Role-based Access Control)
- Row-Level Security (RLS)
- Virtual Private Database (VPD)
- Oracle Label Security (OLS)

Зокрема, віртуальна приватна база даних (VPD) дає змогу обмежувати доступ до даних на рівні рядків і прив'язує політику безпеки до самого об'єкта бази даних. Це дозволяє декільком користувачам мати безпечний прямий доступ до критично важливих даних у межах одного сервера бази даних із забезпеченням повного розмежування даних.

Друге рішення – Oracle Label Security (OLS) – ще одна корисна опція безпеки для бази даних Oracle – фактично дозволяє забезпечити VPD контролем доступу за мітками.

За статистикою більшість зломів сховищ даних здійснюють безпосереднім копіюванням інформації з бази даних або з використанням незахищених резервних чи архівних копій. Інформацію на магнітних носіях захищають здебільшого її шифруванням за алгоритмом AES 256. Якщо дані на носіях інформації зашифровані, то без ключа шифрування зловмисник не зможе їх використати.

Найпоширенішим способом захисту інформації, яка зберігається у сховищі, є "прозоре" шифрування даних. Програму шифрування встановлюють на сервер, до якого безпосередньо під'єднано жорсткі диски. При цьому ключ знаходиться в оперативній пам'яті сервера, а всі дані при їх записуванні на диск автоматично зашифровуються, а при читанні – розшифровуються.

Регламент резервного копіювання та архівування даних встановлюється згідно з вимогами політики безпеки корпорації та відповідно до затвердженого центром обробки даних плану. При плануванні копіювання компонентів сховища даних необхідно оцінювати баланс між рівнем захищеності даних і витраченими на це засобами. Регламент резервного копіювання повинен враховувати вимоги політики безпеки та забезпечити вирішення таких завдань:

– збереження цілісності даних та можливість їх відновлення (точка відновлення);

– збереження доступності даних та можливість відновлення даних у найкоротші терміни (час відновлення);

– довготривале зберігання архівних даних.

Необхідно зазначити, що при зберіганні особливо важливої інформації резервне копіювання всіх даних і серверів доцільно здійснювати на постійній основі. Завдяки цьому дані сховища і будь-який сервер центру обробки інформації можуть бути відновлені за допустимий регламентом проміжок часу. Якщо шифрування даних на жорстких дисках серверів сховища є не завжди виправданим, то для носіїв інформації, що зберігаються поза межами підприємства (резервні копії та архіви на магнітних дисках і стрічках), криптозахист є обов'язковим. Резервні копії даних та їх архіви можуть зберігатись на різних носіях залежно від конкретних вимог. Зазвичай використовують сервер резервного копіювання, який координує процеси копіювання та зберігання створених копій даних.

Для виконання резервного копіювання та відновлення даних використовують спеціальні програмно-апаратні засоби, які забезпечують високу надійність зберігання резервних копій та архівних даних як на дисках, так і на магнітних стрічках. Дискові системи копіювання даних порівняно зі стрічковими забезпечують вищу швидкість довільного доступу до файлів і дозволяють покращити такі важливі параметри, як RPO (період часу, за який сховище може втратити дані), та RTO (період часу, необхідний на відновлення даних). Однак, порівняно зі стрічковими системами дискові системи резервного копіювання мають вищу вартість 1 *Гбайта* інформації.

Стрічкові системи забезпечують вищу швидкість читання і записування порівняно з дисковими. Так, на стрічковий тример формату LTO-6 з урахуванням середнього коефіцієнта компресії 2,5 можна записати до 6,25 *Тбайтів* інформації за швидкості записування 160 *Мбіт/сек*.

Бувають випадки, коли копіювання даних з виконанням паралельного програмного шифрування не забезпечує необхідної продуктивності або взагалі неможливе. Це може бути пов'язано як з недостатньою продуктивністю паралельного шифрування резервних копій даних, так і зі специфікою архітектури та технології побудови сховища. Так, при використанні систем зберігання даних NAS з вбудованою ОС або архітектури типу SAN доцільно застосовувати пристрій захисту Data Fort, вбудований криптопроцесор якого забезпечує шифрування даних на магнітних стрічках зі швидкістю декілька *Гігабітів* на секунду. Проте, вартість таких пристроїв може сягати сотні тисяч доларів.

Резервні та архівні копії даних зберігають у зашифрованому стані на магнітних носіях інформації в спеціально виділеному приміщенні, яке перебуває під охороною. Дублікати архівів найцінніших даних доцільно зберігати в іншому приміщенні.

Висновки

Надійно захистити сховища даних можна лише за умови використання комплексних програмно-апаратних засобів та організаційних заходів.

Контроль доступу до серверної частини сховища висуває вимоги до авторизації та багатофакторної автентифікації користувачів як на рівні операційних і прикладних систем, так і на рівні доступу до операцій з базами даних. Рівень доступу уповноваженим особам як в закриті приміщення центру обробки даних, так і до програмно-апаратних засобів та даних повинен визначатися тільки тим способом і за допомогою тих засобів, які дозволені політикою безпеки.

Політика корпоративної безпеки повинна передбачати застосування багаторівневого незалежного від адміністраторів аудиту подій, що відбуваються на всіх рівнях інформаційної системи. Для централізованого моніторингу подій у режимі реального часу доцільно використовувати системи управління інформацією та повідомленнями безпеки, які забезпечують уповноважений персонал та користувачів мережі інформацією про її стан та дають змогу, відповідно до заданих правил та налаштувань, оперативно реагувати на виникнення загрозливих ситуацій.

Переважно зломи сховищ даних здійснюють безпосереднім копіюванням інформації з бази даних або з використанням незахищених резервних чи архівних копій. Тому захищати дані під час їх записування та зберігання на магнітних носіях необхідно шифруванням.

При зберіганні особливо важливої інформації резервне копіювання всіх даних і серверів доцільно здійснювати на постійній основі. Завдяки цьому дані сховища і будь-який сервер центру обробки інформації можуть бути відновлені за допустимий регламентом проміжок часу.

1. Пасічник В. В., Шаховська Н. Б. Сховища даних: навчальний посібник / В. В. Пасічник, Н. Б. Шаховська. – Львів: "Магнолія 2006", 2008. – 492 с. 2. ISO/IES 27001:2005, Information technology – Security technique – Information security management systems – Requirements. 3. Піскозуб А. З. До питання підвищення рівня захищеності комп'ютерних мереж та систем // Вісник Нац. ун-ту "Львівська політехніка" "Автоматика, вимірювання та керування". – 2012. – №741. – С. 180–183. 4. Alien Vault. Open Source SIEMS (OSSIM) // http://www.alienvault.com/. 5. Security and the Data Warehouseю An Oracle White Paper. April 2005 http://www.oracle.com/ technetwork/middleware/bi-foundation/twp-bi-dw-security-10gr1-0405-128087.pdf

УДК 621.314

А. Г. Павельчак[1], В. В. Самотий[2,3], П. П. Ширий[1]
[1] Національний університет "Львівська політехніка",
кафедра комп'ютеризованих систем автоматики
[2] Politechnika Krakowska im. Tadeusza Kościuszki,
katedra automatyki i technik Informacyjnych
[3] Львівський державний університет безпеки життєдіяльності,
кафедра управління інформаційною безпекою

ПАРАМЕТРИЧНА ОПТИМІЗАЦІЯ СИСТЕМИ КЕРУВАННЯ МОТОРОМ ПОСТІЙНОГО СТРУМУ З ПАРАЛЕЛЬНИМ ЗБУДЖЕННЯМ

Здійснено параметричну оптимізацію для системи керування мотором постійного струму з паралельним збудженням з використанням генетичного алгоритму. Отримано якісні характеристики перехідного процесу системи керування.

Ключові слова: оптимізація, генетичний алгоритм, система керування.

Parametric optimization of control system of DC motor with parallel excitation have done. Optimization have conducted using Genetic Algorithm. Qualitative characteristics of the transition process of control system have obtained.

Key words: optimization, genetic algorithm, control system.

Вступ

Мотори постійного струму мають дуже широку сферу застосування. Це магістральні електровози, робочі мотори на тепловозах, приміські електровози, метрополітени, трамваї, тролейбуси, електромобілі – тобто, там, де потрібні м'які механічні характеристики та широкі межі регулювання. Для транспорту (автомобілі, трактори, літаки тощо), що мають систему живлення на постійному струмі, – всі допоміжні засоби часто приводяться в рух моторами постійного струму. Тому проблема керування швидкістю обертання їх роторів є актуальною. Мотори постійного