УДК 004.05

С.С. Козирєв, к.т.н. (Національний університет кораблебудування, Україна)

ЗАБЕЗПЕЧЕННЯ АПАРАТНОЇ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Побудовано модель апаратних загроз комп'ютерної мережі. Проаналізовано вплив технічних характеристик комп'ютерів та їх модулів на захищеність комп'ютерних мереж. Розглянуто моделі гарантоспроможних (dependability) комп'ютерних мереж. Запропоновано методи і засоби забезпечення апаратної безпеки.

Постійний розвиток, розширення та підвищенням навантаження на об'єкти ком'ютерних мереж викликає необхідність в адекватних та сучасних засобах моніторингу їх технічного стану для забезпечення гарантоспроможності. У зв'язку з розвитком технологій електронних платежів, "безпаперового" документообігу та інших, збій локальних мереж може паралізувати роботу цілих корпорацій і банків, що призводить до відчутних матеріальних втрат.

Захист даних у комп'ютерних мережах стає однією з найгостріших проблем. На сьогодні сформульовано три базові принципи інформаційної безпеки: цілісність даних - захист від збоїв, що ведуть до втрати інформації, а також неавторизованого створення або знищення даних; конфіденційність інформації; доступність для всіх авторизованих користувачів.

При розгляді проблем захисту даних в мережі перш за все виникає питання про класифікацію збоїв, які можуть призвести до знищення або небажаної модифікації даних.

Модель апаратних загроз комп'ютерної мережі виглядає таким чином: збої кабельної системи; перебої електроживлення; побічні випромінювання збої дискових систем; збої систем архівації даних; збої роботи серверів, робочих станцій, мережевих карт і т. д.;

Технічні характеристики комп'ютерів та їх модулів суттєво впливають на захищеність комп'ютерних мереж. Основними модульними складовими комп'ютера є: процесор; материнська плата; оперативна пам'ять (ОЗП); жорсткий диск; cd/dvd пристрій; монітор; відеокарта; звукова карта; мережева картка; блок живлення; usb-пристрої; ups-пристрій.

Захищенність комп'ютерної мережі може бути в деякій мірі забезпечена технічними характеристиками модулів комп'ютера. До захисних характеристик усіх складових можна віднести: апаратний захист від перегріву; додатковий охолоджувальний пристрій; апаратний захист від підвищеної напруги; перевірка контрольної суми даних, що обробляється модулем; додатковий час роботи при максимальному граничному навантаженні; підтримка програмних засобів комунікації з апаратним модулем. Окрім того, модулі, з яких складається комп'ютер повинні мати спеціальні захисні функції для продовження роботи у випадку позаштатних ситуацій. Серед необхідних функцій потрібно виділити: захист за допомогою BIOS, встановлення додаткового охолодження, захист від перенапруги за допомогою UPS.

Існують різні моделі гарантоспроможних (dependability) комп'ютерних мереж, які визначаються міжнародними стандартами в області надійності. Надійність можна розглядати, як таку що складається з трьох елементів: атрибути - спосіб оцінки гарантоспроможності системи; загрози - розуміння речей, які можуть вплинути на гарантоспроможність системи; заходи безпеки - шляхи підвищення гарантоспроможності системи.

Атрибути оцінюють якості системи з точки зору загальної надійності з використанням якісних і кількісних показників, і поділяються на: доступність - готовність до того, щоб коректно функціонувати; надійність - безперервність коректного функціонування; безпечність - відсутність катастрофічних наслідків для користувачів і системного середовища; цілісність - відсутність виконання неналежних зміни системи; відновлюваність - здатність до модифікування та обслуговування. Із вищенаведених атрибутів тільки доступність і надійність обчислюються шляхом прямих вимірювань, а інші є суб'єктивними.

Загрози – події, які можуть вплинути на систему і стати причиною зниження гарантоспроможності. Вони класифікуються наступним чином: проектувальні і концептуальні поми-

лки - це дефекти в системі; помилка під час виконання – це різниця між бажаною поведінкою системи та фактичною; повне виведення з ладу – це стан системи, в якому вона виявляє властивості, які не відповідають або повністю протилежні заявленим специфікаціями.

До засобів забезпечення гарантоспроможності можна віднести: запобігання; видалення; прогнозування; стійкість.

Запобігання має на меті попередження появу або привнесення помилок в систему. Цей засіб виконується на стадії розробки системи та вибору способів реалізації системи.

Помилки видалення можуть бути розділені на дві підкатегорії: видалення в ході розробки та видалення під час використання. Видалення на стадії розробки вимагає постійних тестів та перевірок, для того щоб помилки були знайдені до введення системи в виробниче користування. Як тільки система починає використовуватися, необхідно фіксувати та нотувати помилки з метою виправлення їх під час планових робіт з покращення системи.

Прогнозування передбачає можливі помилки з метою їх подальшого видалення або пом'якшення наслідків, спричинених помилками.

Стійкість забезпечується наявністю механізмів, які дозволять системі здійснювати свої звичні функції навіть за наявності помилок, не зважаючи на те, що якість функцій може бути нижчою.

Заходи забезпечення гарантоспроможності покликані зменшити наявність помилок, які помічає користувач. Знайдені помилки записують за певний проміжок часу та аналізують частоту їхньої появи для виміру ефективності обраних заходів.

Методи і засоби забезпечення апаратної безпеки: аналіз та покращення стану кабельної системи; аналіз та покращення структури системи електроживлення; аналіз та покращення системи резервування та дублювання інформації; створення резерву обладнання на випадок відмови; планування періодичного огляду складових комп’ютерної мережі; моніторинг функціонування мережі з метою визначення поточного стану та прогнозування.

Детальний аналіз вказаних методів показав, що найбільш ефективним є моніторинг функціонування мережі. Система моніторингу повинна забезпечувати постійне спостереження за станом вузлів комп'ютерної мережі: виконувати перевірку доступності мережевих ресурсів і служб, стежити за роботою серверного і комунікаційного обладнання; у разі порушення нормальної роботи повідомляти адміністратора, використовуючи різні засоби оповіщення. Крім відправлення повідомлення адміністратору, система моніторингу може бути налаштована таким чином, щоб проводити обробку подій, тобто відмов у роботі елементів мережі та вживати заходів щодо їх усунення шляхом перезапуску будь-якої програми, виконання заданого сценарію і т.п. Ще один аспект - планування розвитку мережі. Корисно мати на руках статистику що відбулися в мережі подій за тривалий період часу. Такого роду дані допомагають у знаходженні вузьких місць, а також дають ясну і вичерпну картину при аналізі і плануванні змін. Детальна інформація про стан сервісів, вузлів, обладнання економить час адміністратора і допомагає йому у прийнятті рішень. На даний час існує велика кількість програмних комплексів, які використовуються для моніторингу інформаційних мереж, комп'ютерних сервісів, обладнання віддалених комп'ютерів.

Висновки. Аналіз існуючих пропрієтарних моніторингових систем, систем з відкритим кодом, безкоштовних та платних показав, що вони найчастіше занадто складні, бо мають набагато більше функцій, ніж потрібно для задачі технічного моніторингу, а тому потребують значного часу на вивчення документації та встановлення бази даних, вимагають значного збільшення споживання ресурсів, складні в налаштуванні. Таким чином, написання своєї авторської програми для цілей моніторингу технічного стану локальної мережі [1] стає економічно доцільним вирішенням поставленої задачі.

Список літератури

1. Єгоров О.П., Козирєв С.С. Система моніторингу технічного стану комп'ютерної мережі // Матеріали Міжнародної науково-технічної конференції аспірантів, молодих науковців і студентів „Інформаційно-керуючі системи і комплекси”, Миколаїв, 2010. – С. 51-55.