В даний час можливості виконання пошуку за подібністю не використовуються в СУБД. Таким чином, виникає задача розробки алгоритмів виконання спеціальних реляційних операцій, що виникають в задачі ототожнення записів. Проведений аналіз напрямків розвитку сучасних баз даних показує, що склалися і формуються за останні роки тенденції розвитку інформаційних технологій істотно впливають, у тому числі і на функціональні можливості автоматизованих систем. Задача встановлення відповідності між окремими об'єктами - побудова процедур ототожнення в даний час не має задовільного рішення. Побудова процедур ототожнення ускладнюється відсутністю серед загальних атрибутів відповідних один одному таблиць різних БД первинних ключів і наявністю помилок операторського введення. З урахуванням специфіки роботи з персональними даними пропонується вирішення наступних прикладних задач: повна ідентифікація клієнта при наявності спотворень інформації в базі даних або в пошукових запитах; усунення дублікатів записів при надходженні до БД з множинних джерел зі слабоструктурованою інформацією; пошук і коректування помилок в персональних даних клієнтів (фізичних і юридичних осіб).

Список використаних джерел:

1. Гагарина Л. Г. Алгоритмы и структуры данных. / Л. Г. Гагарина, В.Д. Колдаев //— М.:Инфра-М, 2009, - 304 с.

к.т.н., доц. Орленко В.С. (ХмНУ)
к.т.н., с.н.с. Жиров Г.Б. (ВІКНУ
к.т.н., доц. Муляр І.В. (ХмНУ)
Казіміров В.О. (ХмНУ)

Захист від загрозливих програм, заснований на контролі доступу до ресурсів

Однією з важливих задач забезпечення комп'ютерної безпеки є необхідність ефективної протидії загрозливим програмам. У загальному випадку атаки подібних програм можуть бути націлені, як на розкрадання даних, так і на виведення з ладу комп'ютерних ресурсів, як наслідок, об'єктами захисту, стосовно до даних загроз, повинні бути, як інформаційні, так і системні комп'ютерні ресурси. Існуюча статистика зростання загрозливих програм дозволяє припустити про низьку ефективність методів вирішення найбільш актуальних сучасних завдань захисту інформації. Незалежно від типу, загрозливі програми здатні завдавати значної шкоди, реалізуючи будь-які загрози інформації - порушення цілісності, конфіденційності, доступності.

В рамках проведеного дослідження ставиться задача моделювання системи антивірусного захисту з використанням математичного апарату теорії масового обслуговування, визначення і розрахунку основних характеристик з подальшою оцінкою реальної ефективності відомих методів захисту від загрозливих програм.

Проведено дослідження основних типів загрозливих програм, на підставі якого запропоновано класифікацію загрозливих програм за способом

їх виконання. На підставі існуючої статистики зроблено висновок, що найбільш актуальними для захисту є виконувані бінарні і скриптові файли. Проведено дослідження способів впровадження загрозливих програм, в результаті якого дійшли висновку - класи загрозливих програм, що розглядаються передбачають обов'язкове збереження файлу на жорсткому диску перед виконанням (читанням). На основі проведених досліджень всіх типів загрозливих програм пропонується провести їх класифікацію за способами виконання загрозливих файлів. У загальному вигляді загрозливі програми слід ділити на виконувані і макро-програми, в свою чергу виконувані діляться на бінарні, мережні загрозливі програми, класичні комп'ютерні віруси, троянські програми, комп'ютерні черв'яки, хакерські утиліти, потенційно небажане програмне забезпечення, і скриптові загрозливі програми.

Запропоновано загальний підхід до захисту від загрозливих програм, заснований на контролі доступу до ресурсів по розширенням і типам файлів. Дослідження актуальності захисту від загрозливих програм і ефективності існуючих методів захисту, показало, що навіть при такому підході до оцінювання можна зробити висновок, що завдання захисту від загрозливих програм актуальне, а ефективність існуючих засобів захисту низька.

к.т.н. с.н.с. Охрамович М.М. (ВІКНУ)
Доброгурська О.Б. (ВІКНУ)
Галушко С.О. (ВІКНУ)

Концепції побудови систем захисту регламентованої інформації

При реалізації концепції побудови системи захисту, користувач не наділяється елементом довіри, тому що він може вважатися потенційним зловмисником, що і має місце на практиці. Тепер загалом розглянемо концепцію, реалізовану в сучасних універсальних ОС. Тут "власником" файлового об'єкта, тобто особою, що одержує право на завдання атрибутів доступу до файлового об'єкта, є особа, що створює файловий об'єкт. Оскільки файлові об'єкти створюють кінцеві користувачі, тому саме вони й призначають атрибути доступу до створюваних ними файлових об'єктів. Інакше кажучи, в ОС реалізується розподілена схема призначення атрибутів доступу, де елементами схеми адміністрування є власне кінцеві користувачі. У даній схемі користувач повинен наділятися практично такою ж довірою, як і адміністратор безпеки, при цьому нести поряд з ним відповідальність за забезпечення комп'ютерної безпеки. Відзначимо, що централізована й розподілена схеми адміністрування - це дві діаметрально протилежні точки зору на захист, що вимагають зовсім різних підходів до побудови моделей і механізмів захисту. При цьому скільки-небудь гарантований захист інформації можна реалізувати тільки при прийнятті концепції повністю централізованої схеми адміністрування, що підтверджується відомими загрозами ОС. Можливості моделей, методів і засобів захисту будемо розглядати стосовно до реалізації саме концепції централізованого