УДК 004.056.5
К.І. Ільїн, М.І. Ільїн
(Фізико-технічний інститут НТУУ “КПІ”)

МОДЕЛІ І МЕТОДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ОБРОБЦІ В ГРІД СИСТЕМАХ

Ряд важливих прикладних задач пов'язаний з швидкою неперіодичною обробкою великих обсягів персональних даних. Серед прикладів можна назвати популяційні дослідження в медицині та економіці, аналіз соціальних факторів безпеки структурно-складних систем. В даній роботі розглядаються інформаційні технології, моделі та методи побудови економічно-ефективних автоматизованих систем обробки даних в цих задачах.

Необхідність швидкої обробки великих обсягів даних зумовлює використання високопродуктивних обчислювальних систем, неперіодичність навантаження яких робить побудову виділених кластерів економічно невиправданою. Оренда обчислювальних кластерів в ряді задач також не виправдана внаслідок низької якості та малої потужності українських ресурсів (найвищий результат – 41 й 42 місце рейтингу ТОП-50 суперкомп’ютерів СНД станом на 29.03.2011 р.) та законодавчих обмежень на оренду зарубіжних ресурсів для держбюджетних організацій. Наведені проблеми разом з вимогами чинного з 1 січня 2011 року закону про захист персональних даних [1] зумовлюють актуальність дослідження.

Одним з рішень забезпечення обробки великих обсягів даних в умовах обмежень на час реакції та вартість системи обробки є застосування грід технологій. Обчислювальна інфраструктура Українського національного грід (УНГ) об’єднує до 2660 обчислювальних ядер 26 кластерів та надає ресурси безкоштовно. Вимога ст.6 п.9 [1] щодо знеособленого використання персональних даних для історичних, статистичних, наукових цілей, та ст.5 п.2 [1] щодо невіднесення знеособлених персональних даних (ст.2 [1]) до інформації з обмеженим доступом робить можливим для ряду задач обмежитися розробкою комплексної системи захисту інформації для систем збереження, накопичення та знеособлення даних (СЗЗД). В даній роботі пропонується метод побудови СЗЗД на основі Grid Security Infrastructure (GSI, [2]).

Криптографічні елементи механізмів автентифікації, захисту конфіденційності та цілісності, делегування прав, що забезпечуються в GSI в рамках інфраструктури відкритих ключів (PKI), протоколу SSL/TLS та проксі сертифікатів мають бути приведені у відповідність до українського законодавства ([3] та ін.) В основі технічної реалізації GSI (в т.ч. використовуваних в УНГ елементів) лежить бібліотека з відкритим кодом OpenSSL, в рамках якої вже реалізовані подібні російські алгоритми ГОСТ Р 34.10-2001, VKO 34.10-2001, ГОСТ Р 34.11-94, ГОСТ 28147-89 [4], що значно спрощує реалізацію запропонованого підходу.

В доповіді буде представлено результати адаптації елементів GSI до вимог українського законодавства та модель СЗЗД для системи медичних популяційних досліджень електрокардіограм.

1. Закон України “Про захист персональних даних” // Відомості Верховної Ради України від 27.08.2010 - 2010 р., № 34, стор. 1188, стаття 481.
2. Overview of the Grid Security Infrastructure. – http://www.globus.org/security/overview.html
3. Технічні специфікації форматів представлення базових об'єктів національної системи електронного цифрового підпису // Офіційний вісник України від 22.11.2010 - 2010 р., № 87, стор. 166, стаття 3089, код акту 53386/2010.
4. Криптоком OpenSSL – http://www.cryptocom.ru/opensource/.