**УДК 681.3**

**ЗАХИСТ ІНФОРМАЦІЇ У GRID** **ТЕХНОЛОГІЇ**

**Галайчук О.О.**,студент групи ІБ-41*;* **Гриник Р.О.**, викладач

Львівський ДУ БЖД, Львів, Україна

Технологія GRID використовується для створення географічно розподіленої обчислювальної інфраструктури, що об'єднує ресурси різних типів з колективним доступом до цих ресурсів в рамках віртуальних організацій, що складаються з підприємств і фахівців, що спільно використовують ці загальні ресурси.

Розвиток і впровадження технології GRID носить стратегічний характер. У найближчій перспективі ця технологія дозволить створити принципово новий обчислювальний інструмент для розвитку високих технологій в різних сферах людської діяльності.

Ідейною основою технології GRID є об'єднання ресурсів шляхом створення комп'ютерної інфраструктури нового типу, що забезпечує глобальну інтеграцію інформаційних і обчислювальних ресурсів на основі мережевих технологій і спеціального програмного забезпечення проміжного рівня (між базовим і прикладним ПО), а також набору стандартизованих служб для забезпечення надійного сумісного доступу до географічно розподілених інформаційних і обчислювальних ресурсів: окремим комп'ютерам, кластерам, сховищам інформації і мережам[1].

Інфраструктура безпеки GRID (GRID Security Infrastructure – GSI) забезпечує безпечну роботу в незахищених мережах загального доступу (Інтернет), надаючи такі сервіси, як аутентифікація, авторизація, конфіденційність передачі інформації і єдиний вхід в GRID-систему. Під єдиним входом мається на увазі, що користувачеві потрібно лише один раз пройти процедуру аутентифікації, а далі система сама поклопочеться про те, щоб аутентифікувати його на всіх ресурсах, якими він збирається скористатися. GSI заснована на надійній і широко використовуваній інфраструктурі криптографії з відкритим ключем (Public Key Infrastructure – PKI).

Як ідентифікатори користувачів і ресурсів в GSI використовуються цифрові сертифікати X.509. У роботі з сертифікатами X.509 і в процедурі видачі/отримання сертифікатів задіяно три сторони:

* Центр Сертифікації (Certificate Authority – CA)
* Підписчик
* Користувач

Інфраструктура безпеки GRID використовує два типи сертифікатів X.509:

* **Сертифікат користувача** (User Certificate) – цей сертифікат повинен мати кожен користувач, що працює з GRID-системою. Сертифікат користувача містить інформацію про ім'я користувача, організацію, до якої він належить, і центр сертифікації, що видав даний сертифікат.
* **Сертифікат вузла** (Host Certificate) – цей сертифікат повинен мати кожен вузол (ресурс) GRID-системи. Сертифікат вузла аналогічний сертифікату користувача, але він замість імені користувача містить доменне ім'я конкретного обчислювального вузла.

Для забезпечення найвищого рівня інформаційної безпеки GRID пред'являє ряд вимог по безпеці, серед них: множинні інфраструктури безпеки, системи безпеки периметру, ідентифікація, авторизація, шифрування, firewall’и мережевого рівня і додатку, сертифікація [2].

Для розподілених операцій просто необхідне управління і взаємодія з множинними інфраструктурами безпеки. Наприклад, для комерційного банку даних, ізоляція клієнтів усередині цього банку даних – основна вимога, GRID повинен здійснювати не тільки контроль доступу, але і надавати ізоляцію. Як інший приклад, можна привести системи он-лайн розваг, де для пропонованого контенту повинна бути гарантована відповідна ізоляція, такий рівень ізоляції повинен здійснюватися системою безпеки інфраструктури [3].

Загалом інфраструктура захисту інформації в GRID вимагає застосування широко спектру захисних інструментів та методів, що гарантує високу надійність захисту інформації від втрат, несанкціонованого доступу до неї, забезпечення доступності і достовірності даних що передаються.

**ЛІТЕРАТУРА**

1. Foster I., Kesselman C. and Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations // International. J. High Performance Computing Applications. — 2001. — 15(3). P. 200–222. [www.globus.org/research/papers/anatomy.pdf](http://www.globus.org/research/papers/anatomy.pdf).
2. «Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ», НАН України, м. Київ, 2009 р.
3. О. Я. Матов, І. О. Храмова. Перспективні інформаційні технології та розвиток GRID-систем у високопродуктивних глобально-розподілених обчислювальних інфраструктурах корпоративної співпраці, Науково-технічний журнал «Реєстрація, зберігання і обробка даних», м. Київ, 2004 р.