УДК 004.056:004.75
DOI https://doi.org/10.32782/IT/2025-1-32

Максим ШАБАН
кандидат технічних наук, викладач кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, м. Київ, 02121
***ORCID:** 0000-0003-2706-8235*

Наталія ДЯЧЕНКО
кандидат наук з державного управління, доцент кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна, 02121
***ORCID:** 0000-0002-4306-7665*
***Scopus Author ID:** 57216565101*

Любов ЧЕРЕМІСІНА
викладач кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна, 02121
***ORCID:** 0009-0005-0719-0745*

Юрій ЩЕРБИНА
кандидат технічних наук, доцент кафедри інформаційних технологій, Національний університет «Одеська юридична академія», Фонтанська дорога, 23, м. Одеса, Україна, 65009
***ORCID:** 0000-0003-3885-6747*

Бібліографічний опис статті: Шабан, М., Дяченко, Н., Черемісіна, Л., Щербина, Ю. (2025). Аналіз сучасних методів захисту інформації в грід-системах при проведенні державних експертиз КСЗІ. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 244–247, doi: https://doi.org/10.32782/IT/2025-1-32

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В ГРІД-СИСТЕМАХ ПРИ ПРОВЕДЕННІ ДЕРЖАВНИХ ЕКСПЕРТИЗ КСЗІ

У статті досліджено сучасні методи забезпечення інформаційної безпеки в грід-системах, що є основою для проведення державної експертизи комплексних систем захисту інформації (КСЗІ).

***Методологія** роботи полягає у використанні Грід-систем, які відіграють важливу роль у вирішенні складних обчислювальних завдань, що потребують значних ресурсів. Вони дозволяють інтегрувати потужності обчислювальних центрів і розподіляти робочі навантаження між ними. Проте така структура створює нові виклики у сфері безпеки, зокрема щодо захисту даних та ресурсів від несанкціонованого доступу, порушення цілісності та конфіденційності.*

***Метою** статті є розгляд та вдосконалення механізмів, які забезпечують захист в грід-системах, зокрема інфраструктуру Globus Grid Security Infrastructure (GSI), що базується на технології відкритих ключів. Описано її ключові компоненти: протоколи аутентифікації та авторизації, механізми передачі прав доступу, підтримку одноразової автентифікації та використання проксі-сертифікатів X.509. Особливу увагу приділено захисту на рівні повідомлень із використанням стандарту WS-Security та мови SAML для обміну даними про права доступу.*

***Ключові слова:** грід-системи, державна експертиза, комплексна система захисту інформації, Globus GSI, інформаційна безпека.*

Maksym SHABAN
Candidate of Technical Sciences, Lecturer at the Department of Cybersecurity, Information Technologies and Economics, Kyiv University of Intellectual Property and Law of the National University «Odesa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, sabanmaxim@gmail.com
***ORCID:** 0000-0003-2706-8235*

Natalia DIACHENKO
Candidate of Public Administration Sciences, Associate Professor at the Department of Cybersecurity, Information Technology and Economics, Kyiv University of Intellectual Property and Law of the National University "Odesa Law Academy", 210, Kharkivske highway, Kyiv, Ukraine, 02121, n.diachenko@ukr.net
***ORCID:** 0000-0002-4306-7665*
***Scopus Author ID:** 57216565101*

Liubov CHEREMISINA
Lecturer at the Department of Cybersecurity, Information Technology and Economics, Kyiv University of Intellectual Property and Law of the National University "Odesa Law Academy", 210, Kharkivske highway, Kyiv, Ukraine, 02121, cheremisina1112@gmail.com
***ORCID:** 0009-0005-0719-0745*

Yuriy SHCHERBYNA
Candidate of Technical Sciences, Associate Professor at the Department of Information Technologies, National University "Odesa Law Academy", 23, Fontanska doroha, Odesa, Ukraine, 65009, shcherbyna@onua.edu.ua
***ORCID:** 0000-0003-3885-6747*

To cite this article: Shaban, M., Diachenko, N., Cheremisina, L., Shcherbyna, Yu. (2025). Analiz suchasnykh metodiv zakhystu informatsii v hrid-systemakh pry provedenni derzhavnykh ekspertyz KSZI [Analysis of modern methods of information protection in grid systems when conducting state expertise of CIPS]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 244–247, doi: https://doi.org/10.32782/IT/2025-1-32

ANALYSIS OF MODERN METHODS OF INFORMATION PROTECTION IN GRID SYSTEMS WHEN CONDUCTING STATE EXPERTISE OF CIPS

The article investigates modern methods of ensuring information security in grid systems, which are the basis for the state examination of integrated information security systems (IIS). The methodology of the work consists in the use of grid systems, which play an important role in solving complex computing tasks requiring significant resources. They allow to integrate the capacities of computing centers and distribute workloads between them. However, such a structure creates new security challenges, in particular, in terms of protecting data and resources from unauthorized access, breach of integrity and confidentiality.

***The purpose** of the article is to review and improve the mechanisms that provide protection in grid systems, in particular, the Globus Grid Security Infrastructure (GSI), which is based on public key technology. Its key components are described: authentication and authorization protocols, mechanisms for transferring access rights, support for one-time authentication and the use of X.509 proxy certificates. Particular attention is paid to message-level security using the WS-Security standard and the SAML language for exchanging access rights data.*

***Key words:** grid systems, state expertise, comprehensive information protection systems, Globus GSI, information security.*

Актуальність. Сучасні дослідницькі потреби вимагають використання високопродуктивних обчислювальних систем для виконання складних і ресурсомістких завдань. Проте вартість таких систем є досить високою. Як відповідь на ці виклики, з'являються грід-системи, що об'єднують існуючі обчислювальні центри, дозволяють швидко розширювати свої потужності та ефективно виконувати розподілені додатки, залучаючи всі доступні ресурси.

Сьогоднішні методи захисту інформації в комп'ютерних системах базуються на централізованих механізмах, таких як сертифікаційні агенції чи служби авторизації. Однак така модель обмежує використання цих технологій у динамічних умовах, характерних для грід-систем. Це підкреслює актуальність розробки децентралізованих підходів до забезпечення захисту інформації у таких середовищах.

Основи проведення експертизи на відповідність вимогам НД ТЗІ. Швидкий розвиток інформаційних технологій та їх інтеграція в усі аспекти суспільного життя призводять до постійного збільшення кількості загроз для інформаційно-телекомунікаційних систем (ІТС). Особливо критично це для систем, які є складовою частиною об'єктів критичної інфраструктури. Для їх надійної роботи необхідно регулярно тестувати ІТС на предмет вразливостей. Це включає проведення контрольованих дій, що імітують потенційні загрози для виявлення слабких місць у захисті.

Однак недостатньо лише виконати випробування; важливо формалізувати процедуру їх проведення. Для цього в Україні розроблено низку нормативних документів, які регламентують процес тестування. Сукупність заходів з аналізу ІТС отримала назву «Державна експертиза комплексної системи захисту інформації» (КСЗІ).

Метою такої експертизи є перевірка відповідності КСЗІ технічним завданням і нормативним вимогам, а також визначення можливості введення цієї системи в експлуатацію. В Україні державна експертиза КСЗІ проводиться згідно з положенням, затвердженим наказом Адміністрації Держспецзв'язку від 16 травня 2007 року № 93, а також нормативним документом НД ТЗІ 2.6-001-11. Організатором експертизи виступає Держспецзв'язку, який призначається після розгляду відповідної заяви власника інформаційно-телекомунікаційної системи.

Організація інформаційної безпеки грід. У процесі проведення державних експертиз комплексних систем захисту інформації (КСЗІ) було визначено, що грід-системи повинні забезпечувати такі механізми безпеки: аутентифікацію, передачу прав доступу, підтримку одноразового входу, керування життєвим циклом мандатів, авторизацію, забезпечення конфіденційності та цілісності даних, обмін політиками безпеки, проникність через мережеві екрани (firewall) тощо (Cornwall, Jensen, Kelsey, 2004, p. 306). Значна частина цих вимог реалізована у стандарті OGSA (Security Architecture for Open Grid Services), який розроблено Open Grid Forum (OGF). Найпоширенішою реалізацією цього стандарту є Globus Toolkit (GT).

Основними загрозами для інформації у грід-системах залишаються: розкриття даних, порушення їх цілісності, неналежне використання ресурсів та відмова у наданні послуг (Foster, Kesselman, Tuecke, 2001). Захист інформації в грід-інфраструктурі передбачає вирішення двох ключових завдань: забезпечення конфіденційності, цілісності та доступності даних за допомогою організаційних і програмно-технічних засобів, а також відповідність законодавчим вимогам щодо захисту конфіденційної інформації та персональних дані.

Інфраструктура захисту Globus GSI. На сьогоднішній день програмне забезпечення середнього рівня Globus Toolkit фактично стало стандартом для розробки грід-систем. Для забезпечення безпеки ці системи використовують інфраструктуру Globus Grid Security Infrastructure (GSI), що базується на технології відкритих ключів. Протокол GSI (Foster, Kesselman, Tsudik, Tuecke, 1998). виконує автентифікацію користувача в умовах одноразової реєстрації, забезпечує захист комунікацій та підтримує обмежене делегування повноважень.

Одноразова реєстрація дозволяє користувачу проходити автентифікацію лише один раз, створюючи проксі-сертифікат (proxy certificate), який використовується віддаленими службами для виконання дій від імені користувача. Делегування повноважень забезпечує передачу частини привілеїв від одного об'єкта до іншого, що зменшує потенційну шкоду у випадку зловживання сертифікатом.

GSI використовує сертифікати X.509, стандартизовані для інфраструктури відкритих ключів. Для підтримки одноразової реєстрації та делегування було розроблено спеціалізовані проксі-сертифікати X.509. Процедура автентифікації зазвичай базується на протоколі Transport Layer Security (TLS), хоча також можуть використовуватись інші протоколи (Adams, Lloyd, 2002) для роботи з проксі-сертифікатами.

Додатково, розширення GSS-API дозволяють враховувати гетерогенність локальних доменів грід-систем. Розвинена підтримка обмеженого делегування була продемонстрована у прототипах і стала важливою частиною профілю проксі-сертифікатів X.509.

Захист на рівні повідомлень. Захист на рівні транспорту реалізується через відповідні транспортні механізми, які забезпечують базову безпеку грід-сервісів. Однак при інтеграції грід-систем із веб-сервісами використовується захист на рівні повідомлень, що дозволяє контролювати кожне повідомлення SOAP окремо. Це дає змогу адаптувати рівень безпеки залежно від важливості даних.

Специфікація WS-Security забезпечує цілісність даних і конфіденційність, інтегруючи існуючі моделі захисту у повідомлення SOAP. Стандарт SAML (Security Assertion Markup Language) визначає мову та протоколи для обміну інформацією про автентифікацію та права доступу між учасниками грід-систем. Тимчасові мітки SAML сприяють динамічному формуванню довіри між організаціями.

XACML (Extensible Access Control Markup Language) забезпечує узгоджене формування правил доступу, виражених у форматі XML, та дозволяє інтегрувати різні політики безпеки в єдиний набір.

Оцінювання доступності інформації. Однією з важливих задач грід-систем є забезпечення доступності ресурсів і даних. Проте кількість атак на доступність, таких як DoS і DDoS,

стрімко зростає. Основним інструментом для їх реалізації залишаються мережі ботів (botnets), що спричиняють значні збитки організаціям, обмежуючи доступ до критичної інформації.

Для оцінки доступності ресурсів використовується теорія надійності, яка визначає ймовірність працездатності системи у довільний момент часу. На основі цього підходу функціонує програмне забезпечення GridView (Kalmady, Sonvane, Bhatt, 2009), яке дозволяє моніторити доступність грід-сервісів і віртуальних організацій. Хоча GridView збирає дані щогодини, частота оновлення інформації залишається його недоліком.

Висновки. У статті проаналізовано технології захисту інформації в грід-системах, зокрема інструменти Globus Toolkit та Advanced Resource Connector (ARC) NorduGrid 3.0.0. Виявлено слабкі місця у захисті даних, що зберігаються у спільній пам'яті.

На основі аналізу рекомендовано враховувати ці недоліки під час розробки технічних завдань для державної експертизи грід-систем, спрямованих на забезпечення безпеки інформації.

ЛІТЕРАТУРА:

1. Simple Object Access Protocol (SOAP) 1.1. W3C, Note 8, 2000.

2. CMS Requirements for the Grid : Proc. of the Int. Conf. on Computing in High Energy and Nuclear Physics (CHEP2001). K. Holtman. URL: citeseer.ist.psu.edu/article/holtman01cms.html.

2. Foster I., Kesselman C., Tuecke S. The Anatomy of the Grid. Enabling Scalable Virtual Organizations. *International Journal of Supercomputer Applications*, 2001. 15(3), 200–222.

3. Cornwall L.A., Jensen J., Kelsey D.P. Authentication and Authorization Mechanisms for Multi-Domain Grid Environments. *Journal of Grid Computing*, 2004. 9, 301–311.

4. A Security Architecture for Computational Grids: Proc. of ACM Conf. on Computers and Security / Foster, I., Kesselman, C., Tsudik, G., Tuecke, S. 1998. P. 83–91.

5. Adams C., Lloyd S. Understanding PKI: Concepts, Standards, and Deployment Considerations. London, Addison-Wesley. 2002.

6. IETF – Public-Key Infrastructure (X.509) (pkix), 2005. URL: www.tools.ietf.org/wg/pkix

7. IETF – Transport Layer Security (tls), 2005. URL: www.tools.ietf.org

8. Tulloch M. Microsoft Encyclopedia of Security. Redmond, Washington: Microsoft Press. 2003.

9. Kalmady R., Sonvane D., Bhatt K. GridView: A Grid Monitoring and Visualization Tool. 2009. URL: https://twiki.cern.ch/twiki/pub/LCG/GridView/

REFERENCES:

1. Simple Object Access Protocol (SOAP) 1.1. W3C, Note 8, 2000.

2. Holtman, K. (2001). CMS Requirements for the Grid. Proceedings of the International Conference on Computing in High Energy and Nuclear Physics (CHEP2001). Retrieved from: citeseer.ist.psu.edu/article/holtman01cms.html

3. Foster, I., Kesselman, C., & Tuecke, S. (2001). The Anatomy of the Grid: Enabling Scalable Virtual Organizations. *International Journal of Supercomputer Applications*, 15(3), 200–222.

4. Cornwall, L.A., Jensen, J., & Kelsey, D.P. (2004). Authentication and Authorization Mechanisms for Multi-Domain Grid Environments. *Journal of Grid Computing*, 9, 301–311.

5. Foster, I., Kesselman, C., Tsudik, G., & Tuecke, S. (1998). A Security Architecture for Computational Grids. *Proceedings of ACM Conference on Computers and Security*, 83–91.

6. Adams, C., & Lloyd, S. (2002). Understanding PKI: Concepts, Standards, and Deployment Considerations. London : Addison-Wesley.

7. IETF. (2005). Public-Key Infrastructure (X.509) (pkix). Retrieved from: www.tools.ietf.org/wg/pkix

8. IETF. (2005). Transport Layer Security (TLS). Retrieved from: www.tools.ietf.org

9. Tulloch, M. (2003). *Microsoft Encyclopedia of Security*. Redmond, Washington: Microsoft Press.

10. Kalmady, R., Sonvane, D., & Bhatt, K. (2009). GridView: A Grid Monitoring and Visualization Tool. Retrieved from: https://twiki.cern.ch/twiki/pub/LCG/GridView/