© Shaban M. Ukrainian national grid structure from viewpoint of security requirements ensuring in the grid environment // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 1, p. 20-25.

СТРУКТУРА УКРАИНСКОГО НАЦИОНАЛЬНОГО ГРИДА С ТОЧКИ ЗРЕНИЯ ОБЕСПЕЧЕНИЯ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ В ГРИД-СРЕДЕ

Максим Шабан

Институт проблем моделирования в энергетике им. Г.Е. Пухова, Украина

ШАБАН Максим Радович

Год и место рождения: 1988 год, г. Киев, Украина.
Образование: Национальный авиационный университет, 2012 год.
Должность: аспирант ИПМЭ им. Г.Е. Пухова с 2012 года.
Научные интересы: информационная безопасность, прикладное программирование, грид-вычисления.
Публикации: 6 научных публикаций, среди которых научные статьи, тезисы и материалы докладов на конференциях.
E-mail: maximsaban@gmail.com

Аннотация. *Грид-вычисления основаны на совместном и скоординированном использовании различных ресурсов в распределенных виртуальных организациях. Динамичная и многоинституциональная природа грид-среды порождает сложные проблемы безопасности, которые требуют новых технических подходов для своего решения. В этой статье рассмотрен стандарт отрытой архитектуры для грид-сервисов Open Grid Services Architecture (OGSA) с целью определения требований обеспечения безопасности. OGSA - это распределенное взаимодействие и вычислительная архитектура, основанная на сервисах позволяющие обеспечивать совместимость для гетерогенных систем с тем, чтобы различные типы ресурсов могли общаться и обмениваться информацией. OGSA основана на нескольких других технологиях Web -сервисов, таких как Web Services Description Language (WSDL) и Simple Object Access Protocol (SOAP), но перед этой архитектурой поставлена цель быть, в значительной степени, независимой от обработки на уровне транспорта данных. OGSA была разработана как дополнение к архитектуре Web-сервисов специально предназначенных для поддержки грид-требований. Впервые понятие «OGSA» определено в журнале Globus Alliance в статье «The Physiology of the Grid» Яна Фостера, Карла Кесельмана, Джеффри М. Ника и Стивена Тюки, вышедшей в свет в 2002 году. Стандарт был разработан в 2006 году рабочими группами GGF, результатом работы которой стал документ под названием «The Open Grid Services Architecture» версии 1.5.*

Ключевые слова: *грид-системы, грид-вычисления, OGSA, гетерогенные системы, виртуальные организации.*

Вступление

Основным достоинством грид-систем является возможность объединения ресурсов для решения нерегулярно возникающих ресурсоемких вычислительных задач. При этом существует противоречие между желанием получить максимальную производительность и необходимостью обеспечения безопасной работы. Проанализируем современное состояние данной проблемы с целью определения актуальных путей её решения.

Грид-системы первого поколения создавались преимущественно доверяющими друг другу административными единицами — исследовательскими лабораториями и академическими институтами. Globus Alliance (международный консорциум исследователей грид) вместе с другими научными и коммерческими организациями разработал Open Grid Services Architecture (OGSA). Эта архитектура определяет механизмы для создания, именования и обнаружения с грид-служб на постоянной основе.

При создании архитектуры защиты для грид-служб нужно обеспечить поддержку широкого спектра требований к безопасности — от приложений, требующих минимальной защиты или вовсе в ней не нуждающихся, до круга задач, которым необходим высокий уровень конфиденциальности.

Грид-службы содержат различные административные домены, каждый из которых имеет свой автономный механизм защиты. Эффективная архитектура безопасности должна обеспечивать протоколы, позволяющие компенсировать различия между автономными механизмами и при этом предоставлять каждому локальному узлу полный контроль над относящимися к нему ресурсами.

Средства безопасности грид должны поддерживать следующие принципы защиты [1]:

1. Аутентификацию – предоставление способа подключения различных механизмов аутентификации и метода их использования в различных ситуациях.

2. Передачу прав – предоставление средств, позволяющих осуществлять передачу прав доступа от запрашивающей стороны к вызываемой службе.

3. Единоразовый вход – освобождение субъектов, которые выполнили процедуру аутентификации, от необходимости ее повторения при каждой попытке доступа к ресурсам на некоторое время.

4. Жизненный цикл мандатов и его обновление – во многих случаях возможна ситуация, когда процесс, инициированный субъектом, выполняется дольше, чем время действия выданного мандата. Поэтому необходимо предупреждать об этом субъекта либо предусмотреть обновление мандата, для того, чтобы работа могла быть закончена.

5. Авторизацию – разрешение доступа к службам на основании политик авторизации, связанных с ними (кто и на каких основаниях может осуществлять доступ), и предоставление возможности вызывающей стороне задавать политики выполнения (кому клиент доверяет выполнение).

6. Конфиденциальность – предотвращения утечки (разглашения) какой-либо информации.

7. Целостность данных – обеспечение обнаружения несанкционированных изменений.

8. Обмен политиками – предоставление возможности обмена информацией о политиках безопасности вызывающей и вызываемой сторонам для создания безопасной среды обмена информацией.

9. Уровень обеспечения безопасности – реализация средств, позволяющих определить требуемый уровень обеспечения безопасности системы.

10. Проницаемость сетевых экранов (firewalls) – основным барьером при передаче данных в динамических, кроссдоменных грид - систем являются межсетевые экраны, поэтому при проектировании системы необходимо обеспечить возможность свободной передачи данных через экран без изменения их политик безопасности.

Большинство из вышеперечисленных требований вошли в стандарт под названием OGSA (Security Architecture for Open Grid Services), разработанный Open Grid Forum (OGF), и на сегодняшний день Globus Toolkit (GT) является широко распространенной реализацией этого стандарта.

Рассмотрим топологию организации информационной безопасности в Украинском национальном гриде (УНГ) (рис 2).

Основными элементами УНГ являются:

– Ресурсные центры национального уровня.

– Центр сертификации с региональными филиалами.

– Центр регистрации виртуальных организаций.

– Центр мониторинга грид-инфраструктуры и регистрации грид-сайтов.

– Грид-сайты – узлы УНГ, подключены к национальной грид-инфраструктуры.

Координацию роботы для поддержания, функционирования УНГ производит Базовый координационный грид-центр Украинского национального грида и региональные координационные грид-центры.

Рассмотрим основные принципы аутентификации, организацию взаимодействия в грид-среде между пользователем и кластером (рис.1). Аутентификация в грид-системе реализована с использованием программного продукта NorduGrid [2] и задействует сертификат открытого ключа X.509 [3] инфраструктуры открытых ключей [4]. После аутентификации NorduGrid от имени пользователя NorduGrid запускает на идентифицированном кластере распределенный программный продукт пользователя (РППП). Обычно РППП задействует MPI [5] для организации обмена сообщениями в распределённой среде, а конкретный экземпляр РППП исполняется в ОС конкретного узла. РППП, NorduGrid и MPI имеют высокую динамику изменений, поэтому для них нецелесообразно жестко фиксировать требования безопасности. С другой стороны, операционные и сетевые среды имеют традиционные функции и составляют основу безопасности, для них целесообразно жестко регламентировать требования, поскольку от них зависит безопасность функционирования грид-среды в целом.

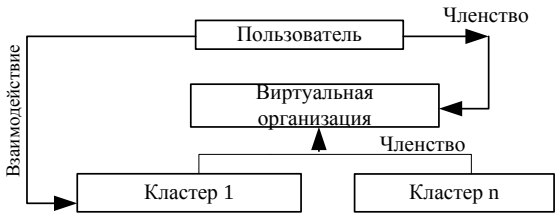

Рис.1 Типовое взаимодействие в грид-среде

На данный момент основной версией промежуточного программного обеспечения (ППО) ARC в УНГ является версия 5.0.2.

Промежуточное программное обеспечение реализует следующие грид-службы (подсистемы): Управление нагрузкой; Управление данными; Информационное обслуживание; Безопасность и контроль прав доступа; Протоколирование; Вычислительный элемент.

Подсистема *управления нагрузкой (Workload Management System, WMS)* осуществляет распределение задач с помощью планировщика / брокера задач, определяет, какой ресурс сейчас свободен, и следит за выполнением заданий, осуществляет фактические операции по управлению задачами: направляет на выполнение, изымает, и т.д, формирует соответствующую среду для выполнения на рабочем узле кластера.

Подсистема *управления данными (Data Management System, MD)* обеспечивает глобальную

файловую систему в масштабах всей грид-инфраструктуры. Она состоит из трех сервисов, поддерживающих доступ к файлам:

– ресурс хранения данных (Storage Element, SE) - совокупность служб, необходимых для обеспечения доступа к файлам, хранящимся на сайте;

– сервис каталогов (Catalog Services, CS);

– планировщик передачи данных (Data Scheduler, DS).

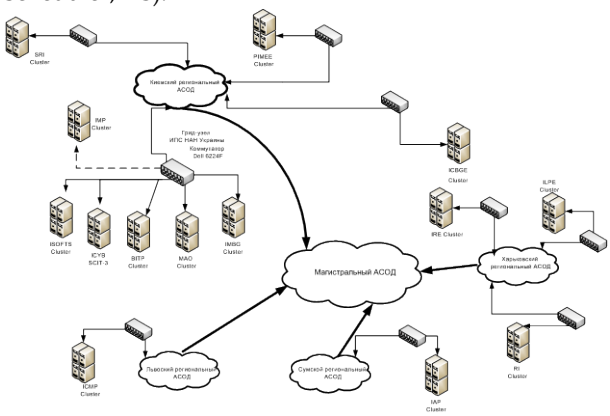

Рис 2. Инфраструктура академического грид

Подсистема *информационного обслуживания (Information System, IS) и мониторинга грид-системы (Relational Grid Monitoring Architecture - R-GMA)* решает задачу сбора и управления данными о состоянии грид-инфраструктуры, получая информацию от множества распределенных источников – поставщиков, предназначена для постоянного контроля функционирования грид-инфраструктуры и обеспечения своевременного реагирования на возникающие проблемы.

Подсистема *безопасности и контроля прав доступа (Grid Security Infrastructure, GSI)* обеспечивает безопасный доступ к ресурсам грид-сайта с учетом прав пользователя и правил обслуживания пользователей данным кластера (такие правила называются «локальной политикой»). Подсистема включает такие сервисы:

– аутентификация – проверка достоверности объекта (пользователя или грид-узла), что направил запрос на выполнение какого-либо действия;

– авторизация – сопоставление объекта и набора прав (привилегий) при работе в грид-инфраструктуре;

– конфиденциальность передачи информации – доступность данных, передаваемых только заранее обусловленном набора объектов;

– целостность передачи информации – неизменность передаваемых данных;

– делегирования прав (имеется в виду, что пользователю нужно только один раз пройти процедуру аутентификации, а дальше система сама обеспечит его подлинности на всех ресурсах, которые он планирует использовать).

Подсистема *протоколирования (Logging and Bookkeeping, LB)* отслеживает выполняемые в разных точках грид-шаги обработки задания, фиксируя и запоминая события, происходящие с ним, такие как запуск, распределение на соответствующий вычислительный элемент, начало выполнения и т.д.

Подсистема *вычислительных элементов (Computing Element, CE)* объединяет вычислительные ресурсы сайта и выполняет функции управления заданиями (запуск, удаление и т.д.), а также поставляет информацию о состоянии ресурсов.

Для определения правил управления доступом к информации, которая функционирует в грид-сайте необходимо определить:

1. Ответственных лиц за установление правил доступа.

2. Состав информации, подлежащей защите.

3. Типы пользователей / групп пользователей, для которых предоставляются права доступа.

4. Варианты возможных прав доступа.

5. Основные правила предоставления доступа.

Политику доступа пользователей к ресурсам грид-сайта, должны определять администратор (менеджер) виртуальной организации, к которой принадлежит пользователь, а также администратор безопасности грид-сайта – владельца ресурсов.

Каждая ВО самостоятельно устанавливает правила работы для своих участников, исходя из соблюдения баланса между потребностями пользователей и имеющимся объемом ресурсов, поэтому пользователь должен обосновать свое желание работать с грид-системой и получить согласие управляющих органов ВО.

Для гибкого управления правами различных пользователей виртуальная организация может определить различные группы пользователей, а отдельным пользователям могут быть приписаны разные роли. Этим различным группам и ролям в процессе авторизации сопоставляются различные права доступа к грид-сервисам (в соответствии с политикой грид-сайтов).

К информации, доступ к которой подлежит управлению, относится:

– информация пользователей;

– технологическая информация.

Программное обеспечение, предназначенное для обработки и защиты этой информации:

– прикладные задачи пользователей;

– ППО, участвующего в обработке информации;

– программное обеспечение по управлению грид-инфраструктурой;

– средства защиты информации.

По уровню полномочий по доступу к информации, связанной с характером и составом работ в грид-сайте выделяются следующие категории:

– пользователь грид-сайта;

– группы пользователей (с одинаковыми правами);

– администраторы грид-сайта.

Для каждой категории устанавливаются полномочия по доступу к файлам и директориям глобального грид-каталога, файлов и директорий ОС грид-сайта.

Согласно ARC и gLite пользователь имеет право работать с файлами только на уровне не выше директории, которая была создана для данного ПО.

В качестве идентификаторов пользователей и ресурсов в GSI используются цифровые сертификаты стандарта X.509 (стандарт международной организации International Telecommunication Union, ITU).

Определим требования к аутентификации, авторизации. В грид-сайте возникают проблемы однозначной аутентификации, авторизации. Пользователи должны работать в безопасном и эффективном грид-среде, для этого должны быть установлены следующие правила:

– взаимодействие между грид-сайтом и другими компонентами грид-инфраструктуры должна быть взаимно подлинности;

– любое действие должно происходить только после соответствующей авторизации – сопоставление объекта осуществляет действие, и набора прав, предоставленных этому объекту для работы в грид-среде.

Аутентификационные решения для грид-сайта должны обеспечивать:

– единственный вход. Пользователь должен зарегистрироваться и аутентифицироваться только один раз в начале сеанса работы, получая доступ ко всем разрешенным ресурсам грид-сайта;

– делегирование прав. Пользователь должен иметь возможность запуска программ от своего имени. Таким образом, программы получают доступ ко всем ресурсам, на которых авторизованный пользователь. Пользовательские программы могут при необходимости делегировать часть своих прав другим программам.

Таким образом, для входа в грид-систему пользователь должен:

1. Иметь персональный цифровой сертификат, подписанный центром сертификации;

2. Быть зарегистрированным хотя бы в одной виртуальной организации;

3. Дать согласие на выполнение правил использования ресурсов грид, изложенными в политике безопасности.

Определим требования к управлению учетными записями пользователей и парольной политикой. Администратор грид-сайта должен обеспечить своих пользователей собственным уникальным идентификатором и паролем (атрибуты) в рамках операционной системы грид-сайта. Выдача или исключения этих атрибутов осуществляется администратором грид-сайта на основании наличия соответствующего сертификата пользователя. Данные атрибуты доступа сообщаются пользователю администратором безопасности грид-сайта.

Политики паролей контролируют безопасность паролей и они могут включать:

– неповторяемость паролей;

– максимальный срок действия паролей;

– минимальный срок действия паролей;

– минимальная длина пароля;

– требования к сложности пароля;

– сохранение паролей.

Пользователям запрещается общее использование атрибутов и разглашение паролей.

Разрешение на доступ может быть заблокирован администратором безопасности в случае возникновения инцидента с пользователем, а срок его действия может определяться сроками профессиональной деятельности, для которой такой доступ был предоставлен. Политики блокировки учетных записей должна быть определена.

Действия по управлению доступом должны регистрироваться в соответствующих журналах, доступ к которым должен контролироваться.

Определим требования к политике по реагированию на инциденты безопасности.

Инцидент безопасности является действием, связанным с нарушением четко установленной политики безопасности.

Управление инцидентами должно предоставлять возможности контролировать опасные действия путем распознавания, фиксации и анализа действий и событий, связанных с соблюдением политики безопасности информации.

Политика по управлению инцидентами должна описывать принятые методы для:

– определения инцидента информационной безопасности, перечень событий, которые являются инцидентами (что в грид-сайте есть инцидентом);

– порядка оповещения ответственного лица о возникновении инцидента (необходимо определить формат отчета, а также отразить контактную информацию лиц, которые должны сообщать об инциденте);

– порядка расследования и устранения инцидента (определение причин инцидента, виновных в возникновении инцидента, порядок сбора и сохранения доказательств);

– реализации необходимых корректирующих и превентивных мероприятий;

– фиксации полной информации об инциденте и корректирующие и превентивные меры.

Процесс управления инцидентами должен быть построен таким образом:

– получения информации об инциденте;

– получение дополнительной информации, связанной с выявленным нарушением;

– анализ ситуации, локализация нарушения и оперативное применение контрмер; установление причин, по которым стало возможным то, что случилось нарушение и, может быть, определение ответственных лиц (расследование);

– проведение профилактических мероприятий, разработка и внедрение мероприятий по недопущению повторного нарушения.

Используемые для выявления инцидентов процедуры сбора информации могут обеспечиваться как техническими, так и организационными мерами, например, в соответствии с требованиями политики безопасности. Сотрудник который выявил нарушения, обязан сообщить о нем администратору безопасности грид-сайта и избегать превышения своих полномочий.

Эффективность процесса управления инцидентами зависит от:

– анализа ситуации, локализации нарушения и оперативного применения контрмер;

– координации и согласованности действий всех вовлеченных в него лиц;

– имеющихся возможностей по получению и анализу информации, связанной с инцидентом;

– оперативности и корректности полученных результатов.

Ответственность за управление инцидентами, связанными с процессами обработки информации, возложена на администратора безопасности.

Минимальный уровень прослеживания для ресурсов грид-сайтов должен обеспечить возможность определить порталы и лиц, которые инициировали работы (выполнение файлов, передачу файлов, экспериментальные работы и т.д.).

Кроме того, для поддержки работающих сервисов необходимо разработать средства управления такие, как мониторинг для выявления действий, нарушающих политику безопасности, и возможность блокировки пользователей, которые инициируют такие действия.

Информация о выявленных инцидентах фиксируется в специальных журналах (в бумажном или электронном виде).

Функции просмотра и анализа журналов, а особенно средств отладки механизмов фиксирования событий, должны быть установлены в политике безопасности.

Определим требования к мониторингу по обеспечению информационной безопасности. Система безопасности также должна содержать средства аудита для поддержки мониторинга в грид-сайте по выявлению неавторизованной деятельности по обработке информации. Средства поддержки аудита должны отслеживать все события, происходящие в системе: ошибки идентификации и аутентификации, попытки атак.

Такое наблюдение за событиями, которые возникают в системе безопасности, позволит обрабатывать все события, связанные с критическими действиями субъектов в системе.

Для обеспечения идентификации и регистрации проблем должны поддерживаться соответствующие журналы регистрации действий администраторов и пользователей, а также неисправностей, возникающих в процессе обработки информации.

Мониторинг системы также должен использоваться для проверки эффективности принятых мер и для верификации их соответствия политике доступа.

Журнал аудита, в котором описывается деятельность пользователей, исключения и события информационной безопасности, должен вестись и храниться в течение согласованного периода для содействия в будущих расследованиях и мониторинга контроля доступа.

Журналы регистрации должны пересматриваться на регулярной основе администраторами грид-сайта.

Средства регистрацию и информация регистрации должны быть защищены от фальсификации и несанкционированного доступа.

Таким образом, мы рассмотрели все стандартные средства, которые призваны обеспечивать надлежащую безопасность в грид-среде и определили требования к: аутентификации, авторизации; управлению учетными записями пользователей и парольной политикой; политике по реагированию на инциденты безопасности; мониторингу по обеспечению информационной безопасности. В свою очередь, государственная экспертиза на соответствие информации циркулирующей в грид-системе является проверкой безопасности на соответствие требованиям, принятым в Украине. За последнее время нами были проведены ряд государственных экспертиз на соответствие информации циркулирующей в грид-системе требованиям нормативных документов систем технической защиты информации в Украине, а именно экспертиза грид-сайта Института теоретической физики им. Н.Н.Боголюбова и экспертиза грид-сервисов Центра регистрации виртуальных организации. Опыт проведения экспертиз показал необходимость унификации документооборота, что позволило бы существенно сократить время необходимое для проведения экспертизы.

Выводы

Анализ существующих тенденций показывает, что актуальным является разработка новых алгоритмов защиты информации адаптированных под требования грид-среды и их экспертиза.

Литература

[1] Foster I., Kesselman C., Nick J., Tuecke S. The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration. – Springer Verlag. – 2002. – 31 p.

[2] Официальный сайт NorduGrid [Электронный ресурс] – 2016 – Режим доступа: http://www.nordugrid.org/.

[3] RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [Электронный ресурс] – 2016 – Режим доступа: https://datatracker.ietf.org/doc/rfc5280/

[4] Мелащенко А.О.Організація кваліфікованої інфраструктури відкритих ключів: монографія / А.О. Мелащенко, О.Л. Перевозчикова; НАН України, Інститутт кібернетики ім. В.М. Глушкова. – К.: Наук. думка, 2010. – 392 с.

[5] MPI-2: Extensions to the Message-Passing [Электронный ресурс] – 2016 – Режим доступа: http://micro.ustc.edu.cn/Linux/MPI/mpi-20.pdf.

УДК 004.056:004.75 (045)

Шабан М.Р. Структура українського національного гріду з точки зору забезпечення вимог безпеки в грід-середовищі

Анотація. *Грід-обчислення засновані на спільному і скоординованому використанні різних ресурсів в розподілених віртуальних організаціях. Динамічна і багатоінстітуціональная природа грід-середовища створює складні проблеми безпеки, які вимагають нових технічних підходів для свого рішення. У цій статті розглянуто стандарт відкритої архітектури для грід-сервісів Open Grid Services Architecture (OGSA) з метою визначення вимог забезпечення безпеки. OGSA - це розподілена взаємодія і обчислювальна архітектура, заснована на сервісах, що дозволяють забезпечувати сумісність для гетерогенних систем для того, щоб різні типи ресурсів могли спілкуватися і обмінюватися інформацією. OGSA заснована на кількох інших технологіях Web-сервісів, таких як Web Services Description Language (WSDL) та Simple Object Access Protocol (SOAP), але перед цією архітектурою поставлена мета бути, в значній мірі, незалежної від обробки на рівні транспорту даних. OGSA була розроблена як доповнення до архітектури Web-сервісів, спеціально призначених для підтримки грід-вимог. Вперше поняття «OGSA» визначено в журналі Globus Alliance в статті "The Physiology of the Grid" Яна Фостера, Карла Кесельман, Джеффрі М. Ніка і Стівена Тюкі, яка вийшла в світ у 2002 році. Стандарт був розроблений у 2006 році робочими групами GGF результатом роботи якої став документ під назвою «The Open Grid Services Architecture» версії 1.5.*

Ключові слова: *грід-системи, грід-обчислення, OGSA, гетерогенні системи, віртуальні організації.*

Shaban M. Ukrainian national grid structure from viewpoint of security requirements ensuring in the grid environment

Abstract. *Grid computing is concerned with the sharing and coordinated use of diverse resources in distributed "virtual organizations." The dynamic and multi-institutional nature of these environments introduces challenging security issues that demand new technical approaches. At this paper we would also describe OGSA. OGSA is a distributed interaction and computing architecture based around services, assuring interoperability on heterogeneous systems so that different types of resources can communicate and share information. OGSA is based on several other Web service technologies, such as the Web Services Description Language (WSDL) and the Simple Object Access Protocol (SOAP), but it aims to be largely independent of transport-level handling of data. OGSA has been described as a refinement of a Web services architecture, specifically designed to support grid requirements. The concept of OGSA is derived from work presented in the 2002 Globus Alliance paper "The Physiology of the Grid" by Ian Foster, Carl Kesselman, Jeffrey M. Nick, and Steven Tuecke. It was developed by GGF working groups which resulted in a document, entitled The Open Grid Services Architecture, Version 1.5 in 2006.*

Key words: *grid system, grid computing, the OGSA, heterogeneous systems, virtual organizations.*

Отримано *17 лютого 2016 року*, затверджено редколегією *10 березня 2016 року*