На правах рукописи

Коноплев Артем Станиславович

МЕТОД КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ В РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург – 2014

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования "Санкт-Петербургский государственный политехнический университет"

Научный руководитель: Калинин Максим Олегович,
доктор технических наук, профессор

Официальные оппоненты: Присяжнюк Сергей Прокофьевич,
доктор технических наук, профессор,
заведующий кафедрой
И6 Оптогеоинформатики
ФГБОУ ВПО "БГТУ "ВОЕНМЕХ"
им. Д.Ф. Устинова"

Томилин Василий Николаевич,
кандидат технических наук,
системный инженер
ООО "Сиско Системс"

Ведущая организация: ФГБОУ ВПО "Петербургский государственный университет путей сообщения"

Защита состоится апреля 2014 г. в часов на заседании диссертационного совета Д212.229.27 при ФГБОУ ВПО "Санкт-Петербургский государственный политехнический университет" по адресу 195251, Санкт-Петербург, ул. Политехническая, 29, Главное здание, а. 175.

С диссертационной работой можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВПО "Санкт-Петербургский государственный политехнический университет".

Автореферат разослан февраля 2014 г.

Ученый секретарь
диссертационного совета

Платонов Владимир Владимирович

Общая характеристика работы

Актуальность. Внедрение функций защиты в распределенные вычислительные сети (РВС) обусловлено ростом числа нарушений безопасности в таких системах (например, инциденты CVE-2009-0046 в Sun GridEngine, CVE-2013-4039 в IBM WebSphere Extended Deployment Compute Grid, связанные с повышением полномочий пользователей). Применение РВС для высокопроизводительной обработки информации ограниченного доступа сопровождается снижением функциональности, в том числе возможности масштабируемости и распараллеливания, вследствие ограничений безопасности, накладываемых на совместное использование ресурсов, связность узлов и перераспределение пользовательских задач. Необходимость в обеспечении защиты информации при минимальных потерях в функциональности РВС – проблема, актуальная для РВС, к которым предъявляются требования функциональной надежности и безопасности: для систем моделирования и обработки операционных данных объектов энергетики, анализа финансовых рисков, проведения ядерных, геоинформационных и крупномасштабных научных экспериментов и исследований, информационно-аналитических систем.

Известными отечественными и зарубежными учеными (В.Ю. Скиба, В.Е. Козюра, В.А. Курбатов, Ю.М. Зыбарев, В.Г. Криволапов, А. Чакрабарти, Ф. Мартинелли, Д. Хоанг, Л. Рамакришнан, Д. Йенсен) проводятся исследования в области моделирования РВС и обеспечения их защиты от внешнего нарушителя, в том числе от угроз распространения вредоносного программного обеспечения. В прикладных продуктах, например, в подсистемах GRAM в РВС Globus Toolkit, CAS в РВС gLite, реализованы механизмы авторизации пользователей для доступа к вычислительным мощностям РВС. В существующих решениях описание и исполнение политик безопасности (ПБ) производятся на множестве виртуальных организаций и фиксированных состояний РВС, что не учитывает распределения прав на уровне вычислительных процессов и высокой интенсивности миграции задач между вычислительными узлами РВС, что приводит к возможности несанкционированного доступа (НСД) к

обрабатываемым данным. Данная работа опирается на результаты указанных исследований и развивает их в следующих направлениях:

– моделирование распределения пользовательских задач по вычислительным узлам РВС в соответствии с требованиями ПБ;

– разработка метода контроля и управления доступом, обеспечивающего в РВС защиту информации от угроз превышения полномочий пользователей.

Разработанная модель распределения пользовательских задач в РВС с соблюдением требований ПБ, а также построенные на ее основе методы и средства позволяют сохранять эксплуатационные характеристики РВС при повышении уровня безопасности информации, в том числе ограниченного доступа, обеспечивают создание защищенных РВС в критически важных отраслях и имеют существенное значение для развития страны.

Цель работы – обеспечение защиты данных, обрабатываемых в распределенных вычислительных сетях, от угроз превышения полномочий пользователей путем разработки метода контроля и управления доступом на основе моделирования распределения пользовательских задач с сохранением функциональных свойств сетей.

Для достижения данной цели в работе решались следующие задачи:

1. Анализ угроз безопасности и механизмов защиты РВС.

2. Построение модели распределения пользовательских задач в РВС, позволяющей описать их параллельное выполнение с учетом отличительных функциональных свойств РВС и задаваемых ограничений доступа к ресурсам.

3. Разработка метода построения карты состояний РВС, позволяющей определять допустимые распределения пользовательских задач в условиях высокой динамики их миграции между узлами РВС.

4. Разработка метода контроля и управления доступом, обеспечивающего защиту информации, обрабатываемой в РВС, от угроз превышения полномочий пользователей и разграничивающего права доступа на уровне пользовательских задач.

5. Разработка архитектуры и реализация системы контроля и управления доступом пользовательских задач к ресурсам РВС.

Научная новизна диссертационной работы состоит в следующем:

– впервые введено понятие ветвящейся раскрашенной функциональной сети Петри, что позволило обеспечить требуемую степень полноты при моделировании безопасного распределения пользовательских задач в РВС с учетом принципов организации распределенных вычислений и предъявляемых требований ПБ;

– разработан метод определения допустимых распределений пользовательских задач в условиях высокой динамики их миграции между вычислительными узлами с использованием деревьев достижимости ветвящихся сетей Петри;

– сформулирована и доказана теорема о безопасности доступа в РВС и на ее основе разработан метод контроля и управления доступом в РВС, обеспечивающий разграничение прав доступа на уровне пользовательских задач.

Практическая ценность работы определяется возможностью использования полученных результатов для автоматизации процедур анализа безопасности научных и коммерческих РВС, для управления и контроля доступа в критически важных РВС, а также для оперативного реагирования на инциденты безопасности в таких системах. Теоретические и экспериментальные результаты работы использованы для подготовки специалистов по защите информации по дисциплине "Безопасность современных высокопроизводительных систем" в ФГБОУ ВПО "СПбГПУ", в НИР "Создание информационно-телекоммуникационных систем высокой доступности и защищенности" (ФЦП "Научные и научно-педагогические кадры инновационной России", 2010-12гг.), при анализе безопасности распределенных вычислительных сетей в СПБГУТ им. М.А. Бонч-Бруевича, создании системы верификации безопасности вычислительных систем в ФГБОУ ВПО "ГУМРФ им. адмирала С.О. Макарова", что подтверждается соответствующими актами об использовании.

Методы исследования. Для решения поставленных задач применены методы системного анализа, теории сетей Петри, теории алгоритмов, теории графов, теории множеств, математического моделирования, математической статистики и математической логики.

Положения, выносимые на защиту:

1. Модель распределения пользовательских задач в РВС на основе ветвящихся сетей Петри.

2. Метод построения карты состояний РВС на основе деревьев достижимости ветвящихся сетей Петри.

3. Теорема о безопасности доступа в РВС, определяющая условия, при которых обеспечивается защита данных, обрабатываемых в РВС, от угроз превышения полномочий пользователей.

4. Метод контроля и управления доступом, обеспечивающий защиту обрабатываемой в РВС информации от угроз превышения полномочий пользователей.

5. Архитектура и система контроля и управления доступом в РВС.

Апробация результатов работы. Основные теоретические и практические результаты работы представлены и обсуждены на межрегиональной конференции "Информационная безопасность регионов России" (Институт информатики и автоматизации РАН, СПб, 2011г.), на научно-технической конференции "Методы и технические средства обеспечения безопасности информации" (СПб, 2012-2013гг.), на Всероссийской научно-методической конференции "Фундаментальные исследования и инновации в национальных исследовательских университетах" (Москва, 2012г.), на международной конференции "РусКрипто’2012" (Москва, 2012г.), на международной конференции Mathematical Methods, Models, and Architectures for Computer Networks Security (MMM-ACNS) (СПб, 2012г.).

Публикации. По теме диссертации опубликовано 16 научных работ, в том числе 2 заявки на выдачу патента РФ на изобретение.

Объем и структура. Диссертация состоит из введения, четырех глав, заключения и списка литературы из 80 наименований.

Содержание работы

Во введении сформулирована и обоснована задача обеспечения защиты информации, обрабатываемой в РВС.

В первой главе представлены результаты исследований угроз безопасности и механизмов защиты РВС. Анализ показал, что функции безопасности РВС не обеспечивают в полной мере защиту обрабатываемой

информации, в том числе от угроз превышения полномочий пользователей.

Специфичные для РВС угрозы безопасности систематизированы по характеру воздействия на РВС, типу последствий и объекту угрозы (рис. 1). Отдельно выделен класс угроз превышения полномочий пользователей, в том числе за счет взаимного влияния пользовательских задач на вычислительных узлах, приводящих к НСД пользователей к данным, обрабатываемым в РВС. Анализ механизмов безопасности в современных РВС (табл. 1) показал, что защита от присоединения к РВС неавторизованных компонентов обеспечивается с помощью механизмов взаимной аутентификации пользователей и провайдеров ресурсов с использованием цифровых сертификатов X.509, шифрования и цифровой подписи информации, передаваемой между узлами РВС.

Рисунок 1 – Систематизация угроз безопасности РВС

Таблица 1 – Механизмы безопасности РВС

Характеристика	**Globus Toolkit**	**UNICORE**	**BOINC**	**gLite**
Взаимная аутентификация	X.509	X.509	Нет	X.509
Применение шифрования транзакций	Да	Да	Нет	Да
Применение цифровой подписи транзакций	Да	Да	Да (в одну сторону)	Да
Авторизация пользователей в РВС	ACL, VOMS, CAS, gridmap	gridmap	gridmap	gridmap, VOMS
Контроль и управление доступом на узлах РВС	Нет	Нет	Нет	Нет

Доступ пользователей к вычислительным мощностям РВС реализуется посредством механизма авторизации пользователей, который включает отображение глобальных идентификаторов пользователей в локальные (например, в подсистеме GRAM в РВС Globus Toolkit версий 1 и 2) и определение пользователей, объединенных в виртуальные организации (ВО) для решения одной вычислительной задачи (например, в подсистеме CAS в РВС gLite).

В существующих системах в процессе предоставления доступа к ресурсам РВС не учитываются отношения доступа, заданные на провайдерах ресурсов, и фактическое распределение прав на уровне пользовательских задач. Это обуславливает возможность влияния пользовательских задач на данные и на задачи других пользователей, исполняющихся на тех же узлах РВС, что приводит к возможности НСД к данным со стороны пользователей РВС. Вследствие этого актуальна задача разработки методов и средств контроля и управления доступом пользовательских задач к обрабатываемой в РВС информации.

Для РВС использование подходов, основанных на представлении системы в виде множества состояний с последующим анализом их безопасности, затруднено в условиях частой миграции параллельно выполняющихся пользовательских задач и "взрыва" числа состояний, количество которых возрастает экспоненциально с ростом числа узлов РВС. Необходима разработка модели, применение которой позволит учесть указанные особенности РВС при обработке информации ограниченного доступа.

Во второй главе представлена модель распределения пользовательских задач в РВС. Модель построена на базе математического аппарата ветвящихся раскрашенных функциональных сетей Петри.

РВС представляется в виде сети Петри $N = (RP,\ T,\ F, M)$, где $RP = \{rp\}$ – конечное множество вершин графа, соответствующих узлам РВС (провайдерам ресурсов), $T = \{t\}$ – конечное множество переходов между вершинами графа, $F = (RP \times T) \cup (T \times RP)$ – отношение смежности вершин, которое задает множество дуг, соединяющих вершины графа и переходы, $M = (m_1, \dots, m_n)$ – маркировка сети, представляющая собой вектор целочисленных значений, n – число узлов РВС (рис. 2).

Пользовательские задачи, исполняемые на узлах РВС, представлены маркерами $m_i \in M$, $1 \le i \le n$. Множество типов маркеров $RT = < C, U >$, где C – класс запрашиваемых пользователем РВС ресурсов (вычислительные ресурсы, пользовательские данные и т.д.), U — множество пользователей РВС. Вид переходов между вершинами графа определяется входной и выходной функциями перехода: $I : RP^n \to T$ и $O : T \to RP^n$.

Модель распределения пользовательских задач в РВС определяется кортежем $\sum = (N, \nu_0, \Psi, J, RT, SP, R)$, где ν_0 – начальное состояние РВС из множества состояний системы $V=\{\nu\}$; J – множество активных задач, каждая из которых сопоставлена с пользователем РВС, который инициировал ее выполнение; SP – требования ПБ; R – текущие отношения доступа на провайдерах ресурсов; $\Psi: N \times J \times RT \times SP \times R \to V$ – функция перехода РВС из состояния в состояние.

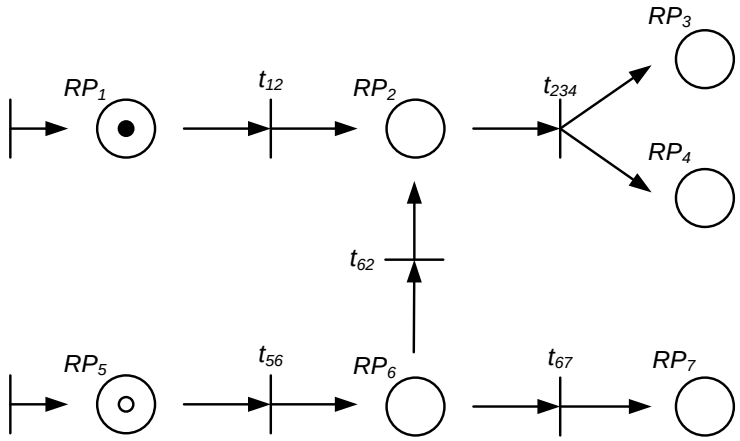


Рисунок 2 – Пример представления РВС с помощью раскрашенной функциональной сети Петри

Комплекс задач по обеспечению защиты данных, обрабатываемых в РВС, от угроз превышения полномочий пользователей включает:

– управление доступом пользователей к обрабатываемым данным – определение множества узлов РВС для выполнения на них пользовательских задач с учетом требований ПБ (известны *J*, *RT*, *SP*, *R*; требуется найти *RP*);

– верификацию требований ПБ – выявление отношений доступа, приводящих к отклонениям от требований ПБ (известны *J*, *RT*, *RP*, *SP*; требуется найти *R*).

Множество субъектов образовано пользователями РВС (*U*). Множеством объектов являются информационные и вычислительные ресурсы РВС. Для $\forall ResProv \in RP$ определен список существующих на нем локальных учетных записей *LocalUIDList*. Также определена функция *GetLocalUIDList*, позволяющая получить данный список для определенного провайдера ресурсов. Для $\forall ResProv \in RP$ определена функция *MapUserToUID*: $<RP, U> \rightarrow LocalUIDList$, отображающая множество пользователей РВС в локальные учетные записи *ResProv*.

Пользователю *User* разрешается доступ к вычислительным ресурсам провайдера ресурсов *ResProv*, если успешно пройдена процедура взаимной аутентификации, для *ResProv* определена локальная учетная запись, в которую отображаются пользователи РВС, и данный тип доступа разрешен требованиями ПБ:

$$\begin{aligned} &HasCompAccessRight(User, ResProv, SP) \\ &= (IsTrustedByU(User, ResProv) \wedge \\ &IsTrustedByRP(ResProv, User) \wedge \\ &(MapUserToUID(ResProv, User) \neq \emptyset)) \wedge \\ &IsAccessAllowedBySP(User, ResProv, SP). \end{aligned} \quad (1)$$

Применительно к информационным ресурсам РВС, локальная учетная запись на узле, в которую отображаются пользователи РВС, должна дополнительно иметь право доступа *Right* к объекту файловой системы *Object*:

$$\begin{aligned} &HasFSOAccessRight(User, ResProv, SP, Object, Right) \\ &= IsTrustedByU(User, ResProv) \wedge \\ &IsTrustedByRP(ResProv, User) \wedge \\ &(LUser = MapUserToUID(ResProv, User) \wedge (LUser \neq \emptyset) \wedge \\ &IsAccessAllowedBySP(User, ResProv, SP) \wedge \\ &HasLocalAccessRight(LUser, ResProv, Object, Right). \end{aligned} \quad (2)$$

Начальная маркировка сети Петри, описывающей любую РВС – $M_0 = (m_1, \dots, m_n)$. Каждый маркер данной маркировки принимает значение в интервале от 0 до n_A, где n_A – количество активных узлов РВС, с которых пользователи РВС могут инициировать создание задачи при условии, что сделать это, не получив результата исполнения предыдущей задачи, нельзя ($n_A \leq n$). Общее число состояний, описывающих такую

РВС, – $n_A{}^n$ (например, при n = 1000 мощность множества состояний составляет 10^{3000}). Для уменьшения пространства состояний построенной модели в работе применяется метод частичного порядка.

Определение 1. Ветвящаяся сеть Петри – функциональная раскрашенная неограниченная сеть Петри, в которой существуют только простые (Т-) переходы и разветвления (F-переходы).

Ветвящиеся сети Петри – подкласс Е-сетей, которые представляют собой расширение математического аппарата раскрашенных сетей Петри. В работе показано, что любая РВС моделируется ветвящейся сетью Петри.

Теорема 1 (теорема об эквивалентности маркировок). Любая маркировка ветвящейся сети Петри $N = (RP, T, F, M)$, достижимая из маркировки M, также достижима из маркировки $M' = (m'_1, \ldots, m'_n)$, $m_i' = \{0, 1\}$, полученной в результате применения к N частичного порядка, равного единице.

Доказательство теоремы определяется отсутствием циклических блокировок в ветвящейся сети Петри, и тем, что количество маркеров в каждой позиции не влияет на условие срабатывания переходов. Эквивалентность маркировок позволяет сократить мощность пространства состояний модели, описывающей произвольную РВС, до 2^n состояний.

В третьей главе предложен метод построения карты состояний РВС на основе деревьев достижимости ветвящихся сетей Петри и разработан метод контроля и управления доступом в РВС.

Метод построения карты состояний РВС основан на решении задачи достижимости ветвящейся сети Петри, моделирующей РВС. Для заданной ПБ SP и ветвящейся сети Петри $N = (RP, T, F, M)$ с начальной маркировкой $M_0 = (m_1, \ldots, m_n)$ строится дерево достижимости, где в качестве вершин выступают маркировки с минимальным частичным порядком. Такое дерево является конечным и согласно теореме 1 эквивалентно дереву достижимости исходной сети Петри, моделирующей РВС. Вершины полученного дерева образуют множество состояний, в которые может перейти РВС.

Определение 2. Безопасным по доступу состоянием РВС называется состояние $\nu \in V$, в котором для ветвящейся сети Петри $N = (RP, T, F, M)$, описывающей данную РВС, и для заданных множеством SP

требований ПБ $\forall m \in M$, $\forall Job \in J$ и $\forall ResProv \in RP$, одновременно выполняются условия:

1. $GetJobType(Job) \in RT^k, k \in \{1, \dots, l\}, l = |RT|$,
2. $AllowedSPRights(SP, JobToU(Job), ResProv) \in RT$,

где функция $GetJobType : J \to RT$ возвращает тип пользовательской задачи, а функция $JobToU : J \to U$ — идентификатор пользователя, инициировавшего данную задачу.

В безопасном состоянии на каждом узле РВС существуют только те отношения доступа, тип которых разрешен требованиями ПБ.

Теорема 2 (теорема о безопасности доступа в РВС). РВС в данном состоянии безопасна по доступу тогда и только тогда, когда безопасны по доступу данное состояние и все достижимые состояния, являющиеся узлами дерева достижимости ветвящейся сети Петри, моделирующей данную РВС.

Метод контроля и управления доступом в РВС состоит в сопоставлении прав доступа, запрашиваемых пользовательской задачей, с требованиями ПБ и фиксировании узлов РВС, на которых данный тип доступа разрешен. Для каждого зафиксированного узла РВС запрашиваемые права доступа сопоставляются с текущими правами доступа, заданными для всех пользователей на данном узле. В результате формируется множество узлов РВС, на которых допустимо выполнение пользовательской задачи с учетом требований ПБ. На узлы РВС передаются правила нового распределения задач, тем самым корректируется вид выходной функции перехода (рис. 3).

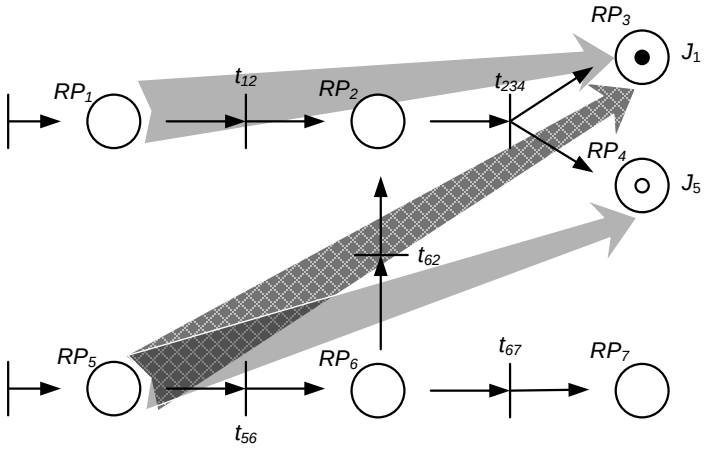


Рисунок 3 – Схема распределения пользовательских задач
в соответствии с требованиями ПБ

Предложенный метод контроля и управления доступом в РВС позволяет верифицировать требования ПБ путем применения к каждому состоянию функций проверки (1) и (2).

В четвертой главе представлена архитектура системы контроля и управления доступом пользовательских задач к вычислительным ресурсам РВС, и представлены результаты оценки эффективности ее работы.

Система контроля и управления доступом в РВС имеет централизованную архитектуру (рис. 4) и включает агенты сбора параметров, формирующие описание текущего состояния РВС, и подсистему анализа безопасности РВС, которая реализует управление доступом пользовательских задач к узлам РВС и верификацию требований ПБ. Архитектура системы обеспечивает совместимость со сторонними автоматизированными системами управления и мониторинга РВС (заявка №2013118953 на выдачу патента РФ на изобретение).

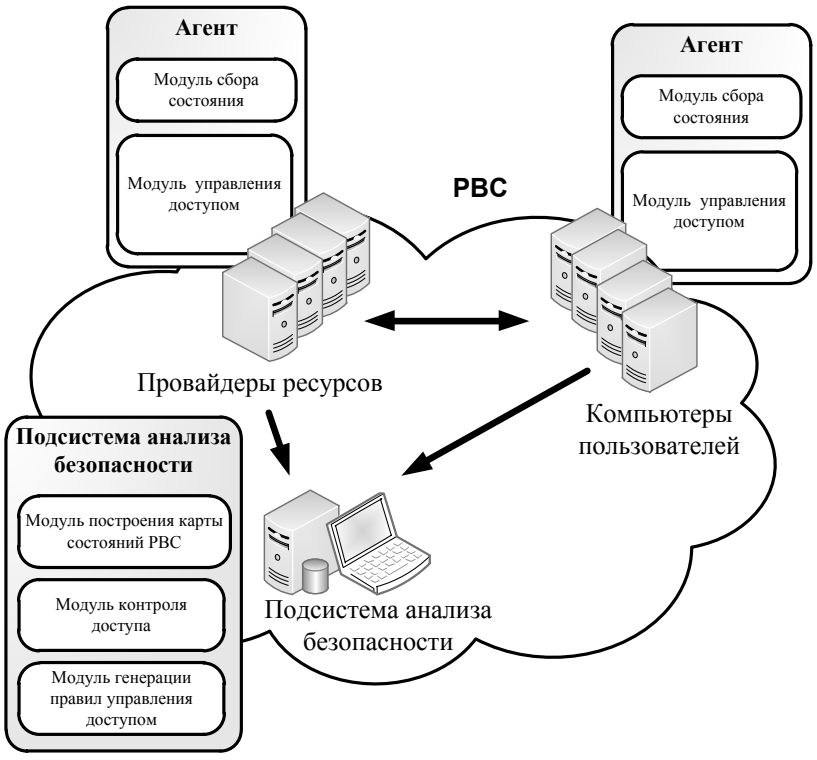


Рисунок 4 – Архитектура системы контроля и управления доступом в РВС

Программные агенты выполняют сбор параметров системы (множества активных пользовательских задач, текущих отношений доступа на узлах РВС, сертификатов пользователей и узлов РВС, типов и параметров авторизации). Информация о состоянии узлов РВС передается в подсистему анализа безопасности. Модуль построения карты состояний

формирует дерево достижимости ветвящейся сети Петри, моделирующей РВС, и рассчитывает последовательность смены состояний РВС. В соответствии с предложенным в работе методом модуль контроля доступа применяет к каждому состоянию функцию проверки выполнения требований ПБ (заявка №2013135959 на выдачу патента РФ на изобретение). Модуль генерации правил управления доступом определяет вид выходной функции перехода для каждого узла РВС и формирует правила управления доступом пользовательских задач. Посредством модулей управления доступом указанные правила применяются на провайдерах ресурсов.

В работе проведена оценка эффективности предложенного метода для обеспечения защиты информации ограниченного доступа, обрабатываемой в РВС, в условиях сохранения их функциональных свойств. В качестве показателя эффективности выступает снижение временных затрат на обработку информации по сравнению с применением организационных мер, заключающихся в разделении РВС на множество слабосвязанных сегментов.

Испытания проведены на лабораторном стенде из 300 вычислительных узлов, представляющих собой виртуальные машины многопроцессорной ЭВМ под управлением Xen Cloud Platform. По результатам 10000 проведенных испытаний с переменным числом узлов для РВС, в состав которой интегрирована разработанная система контроля и управления доступом, успешных реализаций угроз превышения полномочий пользователей не зафиксировано. Число реализованных угроз, до и после применения разработанной системы, представлено на рис. 5.

Общее время T, необходимое для выполнения пользовательской задачи в РВС, рассчитывается по формуле $T = t_{\text{о}} + t_{\text{п}} + t_{\text{б}}$, где $t_{\text{о}}$ – время обработки задачи n узлами РВС, $t_{\text{п}}$ – время передачи всей необходимой для расчетов информации на n узлов РВС, $t_{\text{б}}$ – время, затрачиваемое на определение допустимых распределений пользовательских задач в соответствии с предложенным в работе методом.

Время обработки задачи n узлами РВС (в соответствии с законом Амдала) $t_{\text{о}} = k_1 * (k_2 + \frac{1-k_2}{n})$, где k_1 – общее время выполнения задачи одним узлом, k_2 – доля нераспараллеливаемого кода задачи.

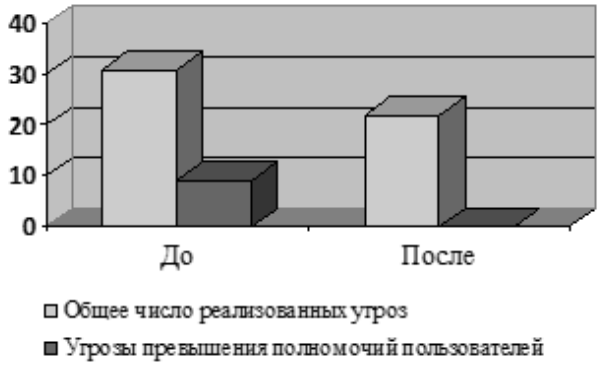


Рисунок 5 – Оценка безопасности РВС

Время передачи информации на n узлов РВС $t_{\text{п}} = n\,\frac{k_3}{k_4}$ и время определения допустимых распределений пользовательских задач $t_{\text{б}} = \frac{k_5 \cdot 2^n}{k_6}$, где k_3 – объем необходимых для вычислений данных, передаваемых на каждый узел РВС, k_4 – скорость передачи данных между узлами РВС, k_5 – число операций, необходимых для верификации безопасности состояния РВС, являющегося узлом дерева достижимости ветвящейся сети Петри, k_6 – пиковая вычислительная мощность узла РВС.

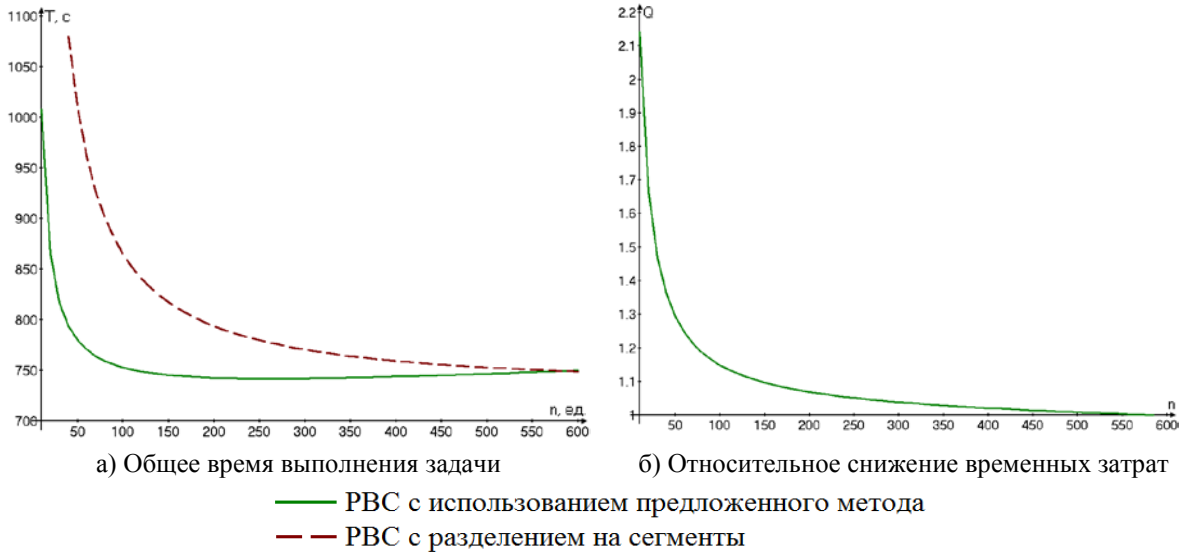
Относительное снижение временных затрат на обработку информации ограниченного доступа в РВС при использовании предложенного метода:

$$Q = \frac{\sum_{i=1}^{d} T_i}{\sum_{i=1}^{d} T_i'} = \frac{\sum_{i=1}^{d} (k_{1i} \cdot \left(k_2 + \frac{(1-k_2)c}{n}\right) + \frac{n}{c} \cdot \frac{k_3}{k_{4i}})}{\sum_{i=1}^{d} (k_{1i} \cdot \left(k_2 + \frac{1-k_2}{n}\right) + n\frac{k_3}{k_{4i}} + \frac{k_5 \cdot 2^n}{k_{6i}})}, \quad (3)$$

где T_i и T_i' – общее время, необходимое для выполнения задачи в РВС, с применением предложенного в работе метода и без, соответственно; c – число категорий информации ограниченного доступа, обрабатываемой в РВС, d – число итераций по выполнению пользовательской задачи в РВС.

Типовые решаемые задачи в РВС, на базе которых строятся современные системы моделирования и обработки операционных данных объектов энергетики и ядерных исследований, имеют следующие характеристики: $k_1 \approx 1$ час, $k_2 \approx 20\%$, $k_3 \approx 512$ Кб, $k_4 \approx 100$ Мб/с, $k_5 \approx 10^2$ опер, $k_6 \approx 4 * 10^{10}$ опер/с, $n \approx 500$, $c = 5$. Полученные экспериментальные результаты для РВС с указанными характеристиками представлены на рис. 6.

Внедрение системы контроля и управления доступом в РВС обеспечивает защиту обрабатываемых данных от угроз превышения полномочий пользователей, одновременно позволяет сократить временные затраты, связанные с оценкой безопасности, и тем самым увеличить относительную производительность РВС, обрабатывающих информацию ограниченного доступа.



а) Общее время выполнения задачи б) Относительное снижение временных затрат

Рисунок 6 – Экспериментальные результаты оценки эффективности предложенного метода

Разработанный метод и его реализация в совокупности с применяемыми в современных РВС механизмами безопасности обеспечивают защиту обрабатываемой информации при условии сохранения функциональных свойств РВС.

В заключении приведены результаты и выводы, полученные в ходе выполнения работы.

В работе получены следующие основные результаты:

1. Систематизированы специфичные для РВС угрозы безопасности, выделен класс угроз превышения полномочий пользователей, приводящих к НСД пользователей к данным, обрабатываемым в РВС.

2. Введено понятие "ветвящиеся раскрашенные функциональные сети", дополняющее математический аппарат сетей Петри, что позволило разработать модель распределения пользовательских задач в РВС и сократить мощность пространства состояний данной модели.

3. Разработан метод построения карты состояний РВС на основе деревьев достижимости ветвящихся сетей Петри, что позволило выполнять оценку безопасности состояний РВС и определять допустимые распределения пользовательских задач с учетом их миграций между вычислительными узлами РВС.

4. Сформулирована и доказана теорема безопасности доступа в РВС, определяющая условия, при которых обеспечивается защита данных, обрабатываемых в РВС, от угроз превышения полномочий пользователей, и на ее основе разработан метод контроля и управления доступом в РВС, позволяющий верифицировать требования ПБ и корректировать вид выходной функции перехода путем передачи на узлы РВС правил распределения пользовательских задач.

5. Построена архитектура и разработана система контроля и управления доступом в РВС, обеспечивающая защиту данных, обрабатываемых в РВС, от угроз превышения полномочий пользователей.

Основные результаты диссертационной работы изложены в 16 печатных трудах. Ниже приведены основные из них:

1. Коноплев, А.С. Верификация требований политик информационной безопасности в системах распределенных вычислений / А.С. Коноплев, М.О. Калинин // Системы высокой доступности. – 2012. – №2. – т. 8. – С. 63-67.

2. Коноплев, А.С. Формализация комплекса задач по обеспечению защиты ресурсов грид-систем от несанкционированного доступа / М.О. Калинин, А.С. Коноплев // Проблемы информационной безопасности. Компьютерные системы. – 2012. – №2. – С. 7-13.

3. Konoplev, A.S. Security Modeling of Grid Systems using Petri Nets / Peter D. Zegzhda, Dmitry P. Zegzhda, Maxim O. Kalinin, Artem S. Konoplev // Lecture Notes in Computer Science. – Springer-Verlag Berlin Heidelberg, 2012. – P. 299-308.

4. Способ проверки прав доступа для учетных записей пользователей в грид-системах и система для его осуществления : заявка №2013135959 Рос. Федерация : МПК G06F7/00 / А.С. Коноплев, М.О. Калинин – заявл. 30.07.2013 – 1 с.

5. Способ доверенной интеграции систем управления активным сетевым оборудованием в распределенные вычислительные системы и система для его осуществления : заявка №2013118953 Рос. Федерация :

МПК G06F7/00 / А.С. Коноплев, М.О. Калинин, Д.П. Зегжда – заявл. 23.04.2013 – 1 с.

6. Коноплев, А.С. Защита высокопроизводительных вычислительных сетей на основе автоматического управления доступом заданий к вычислительным узлам / А. С. Коноплев // Межрегион. конф. «Информационная безопасность регионов России (ИБРР-2013)» : мат-лы конф. – Спб. : СПОИСУ, 2013. – С. 103-103.

7. Коноплев, А.С. Противодействие кибератакам на информационные ресурсы грид-систем / А.С. Коноплев // Науч.-техн. конф. "Методы и технические средства обеспечения безопасности информации" : мат. конф. – СПб.: Изд-во Политехн. ун-та. 2013. – С. 97-99.

8. Коноплев, А.С. Анализ механизмов обеспечения информационной безопасности в грид-системах / А.С. Коноплев // Науч.-техн. конф. "Методы и технические средства обеспечения безопасности информации" : мат-лы конф. – СПб.: Изд-во Политехн. ун-та. 2012. – С. 105-107.

9. Коноплев, А.С. Способ модельного представления механизмов защиты грид-систем / М.О. Калинин, А.С. Коноплев // Межд. науч.-практич. конф. "Информационная безопасность-2012" : мат-лы конф. Ч. 1. – Таганрог: Изд-во ТТИ ЮФУС. 2012. – С. 51-57.

10. Коноплев, А.С. Поддержание защищенности информационных и вычислительных ресурсов в грид-системах / А.С. Коноплев, М.О. Калинин // Науч.-техн. конф. "Методы и технические средства обеспечения безопасности информации" : мат-лы конф. – СПб.: Изд-во Политехн. ун-та. 2012. – С. 107-110.

11. Коноплев, А.С. Обеспечение высокой защищенности информационно-телекоммуникационных систем распределенных вычислений / А.С. Коноплев // Всерос. научн.-методич. конф. "Фундаментальные исследования и инновации в национальных исследовательских университетах" : мат-лы конф. – СПб.: Изд-во Политехн. ун-та. 2012. – С. 83-84.

12. Коноплев, А.С. Верификация безопасности в грид-системах / М. О. Калинин, А. С. Коноплев // Наука и общество. Наука и прогресс человечества» : тез. секц. докл. СПб науч. форума ; VII Петербургская встреча лауреатов Нобелевской премии ; СПб акад. ун-т – науч.-обр. центр нанотехнологий РАН. – СПб. : Изд-во Политехн. ун-та, 2012. – С. 153-154.

13. Коноплев, А.С. Анализ выполнения политик информационной безопасности в Grid-системах / М. О. Калинин, А. С. Коноплев, Я. А. Марков // Науч.-техн. конф. "Методы и технические средства обеспечения безопасности информации" : мат-лы конф. – СПб. : Изд-во Политехн. ун-та. 2011. – С. 143-146.