АНАЛИЗ ВОПРОСОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ПРИМЕНЕНИЯ ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

К.Н. Цебренко, *канд. техн. наук, доцент*
Академия маркетинга и социально-информационных технологий – ИМСИТ (Россия, г. Краснодар)

DOI: 10.24411/2500-1000-2020-10940

Аннотация. *Важным вопросом обеспечения информационной безопасности для высокопроизводительных вычислений является использование виртуализации и облачных вычислений. Данный подход создал много новых рисков безопасности, которые нужно изучить. В статье рассмотрен вопрос использования криптографических методов защиты для достижения безопасности данных в облачных системах на базе алгоритма ГОСТ 28147-89. Исследованы вопросы, связанные безопасностью данных и информация о контексте HPC во время организации доступа к услугам и ресурсам. Рассмотрено использование и реализация криптографического алгоритма ГОСТ 28147-89. Предложены изменения в алгоритме ГОСТ 28147-89: включен генератор случайных чисел для формирования ключа в виде случайного числа. Он использован как ключ для шифрования и дешифрования в рамках одной сессии. Этот метод опробирован при создании прототипа по предложенной концепции на вычислительном кластере Академии маркетинга и социально-информационных технологий – ИМСИТ.*

Ключевые слова: *анализ, системы безопасности, шифрование, высокопроизводительные вычислительные системы, генератор, ключ.*

Высокопроизводительные вычислительные системы становятся одной из самых динамично развивающихся в мире технологий в IT области. Организации все чаще используют высокопроизводительные вычислительные системы (HPC) для улучшения операционной эффективности, сокращения расходов и наращивания вычислительных мощностей автоматизированных информационных систем [1]. Использование суперкомпьютера, размещенного в определенном месте и подключенного к сети Интернет, позволяет уменьшить вычислительную мощность рабочих станций и сделать систему централизованной. Высокопроизводительные вычислительные системы также можно использовать для создания веб-и файл-серверов и применения облачных вычислений. Однако, использование централизованной системы накладывает более серьезные требования к информационной безопасности [2]. В этой связи, рассмотрим вопросы безопасности данных и информации в контексте использования HPC (High-performance computing).

Одним из вопросов обеспечения информационной безопасности для высокопроизводительных вычислений является использование виртуализации и облачных вычислений. Этот подход создал много новых рисков безопасности, которые еще предстоит изучить. Мы предлагаем рассмотреть вопрос использования криптографических методов защиты для достижения безопасности данных в облачных системах. Рассмотрим вариант реализации криптозащиты на базе алгоритма ГОСТ 28147-89 [3]. Анализ предлагаемого метода показывает, что он после внедрения может привести к положительному результату. Алгоритм необходимо реализовать в облаке, созданном в проекте HPC системы, как службу внутри кластера.

Внутренний обмен данными между кластерами играет жизненно важную роль. Мы использовали метод, который уже существует в данных систем связи, и реализовали шифрование данных методом ГОСТ 28147-89. Алгоритм ГОСТ 28147-89 представляет собой блочный шифр с 256-битным ключом и 32 циклами преобразования, оперирующий 64-битными блоками. Основа алгоритма шифра — сеть Фейстеля (рис. 1).

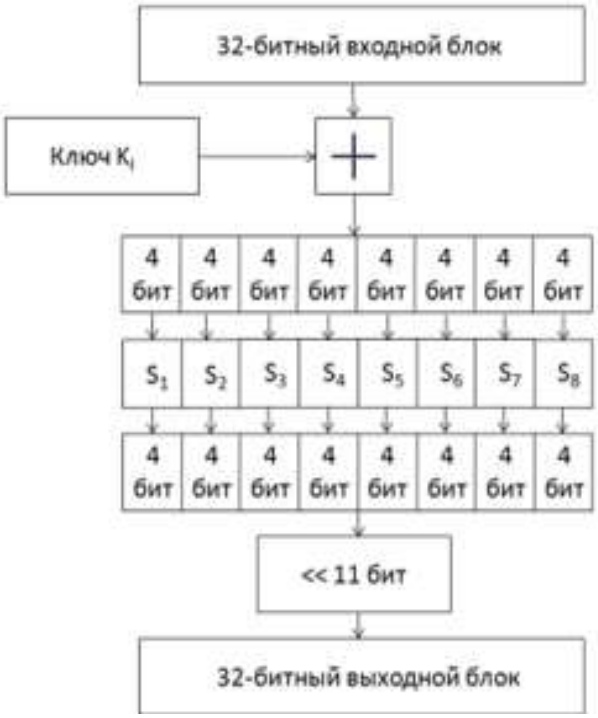

Рис. 1. Функция f(Ai, Xi), используемая в сети Фейстеля

При реализации ГОСТ 28147-89 в высокопроизводительных вычислительных системах используем дополнительно генератор случайных чисел. Он будет генерировать случайные числа в качестве ключа Ki.

Всякий раз, когда конкретный пользователь будет входить в HPC для доступа к сервису, генератор случайных чисел будет генерировать число, которое является ключевым значением для криптоалгоритма. Этот ключ будет оставаться в течение сеанса у данного пользователя, пока он не покинет систему. Каждый раз процесс шифрования и дешифрования происходит за один сеанс, с данным ключом. Если, одновременно, любой другой пользователь входит в систему, генератор случайных чисел будет предоставлять другой ключ к алгоритму ГОСТ 28147-89 при реализации данного протокола в HPC. Большое количество пользователей может использовать одинаковые или разные кластеры для хранения и обработки данных, при этом активный ключ сессии приведет к повышению уровня безопасности.

После создания прототипа по предложенной концепции на вычислительном кластере Академии маркетинга и социально-информационных технологий – ИМСИТ (суперкомпьютер на базе узлов 2xXeon EM64T 2.333 GHz 4 GB RAM, суммарная мощность которого составляет 1,2 TFlops), было установлено, что метод показывает хороший результаты. Дальнейшие исследования будут направлены на разработку комплексной системы безопасности кластера.

Таким образом, использование высокопроизводительных вычислительных систем позволяют получать доступ к информации и вычислительным ресурсам с более высокой скоростью и с большей стабильностью. Использование таких вычислительных ресурсов может быть доступно в любое время и в любом месте через удаленный доступ. При этом обеспечение информационной безопасности является одним из важных вопросов в случае обмена информацией и данными между различными пользователями. Основные трудности возникают из-за параллельной работы. Данный подход можно, например, использовать при шифровании информации передаваемой по радиоканале [4-5] или при использовании проводных линий связи. В этой статье рассмотрены вопросы, связанные безопасностью данных и информация

о контексте HPC, особенно, во время организации доступа к услугам и ресурсам. Рассмотрено использование и реализация криптографического алгоритма ГОСТ 28147-89. Внесены небольшие изменения в алгоритме ГОСТ 28147-89 – включили генератор случайных чисел для генерации ключа в виде случайного числа. Он использован как ключ для шифрования и дешифрования в рамках одной сессии. Этот метод использован при создании прототипа по предложенной концепции на вычислительном кластере Академии маркетинга и социально-информационных технологий – ИМСИТ.

Библиографический список

1. Фролов Р.Н. Моделирование процесса тепломассопереноса в капиллярно-пористом теле с использованием параллельных вычислений // Известия вузов. Пищевая технология. – 2012. – №1. – С. 79-83.

2. Anirban Mitra, Ramanuja Nayak. Studying Security Issuesin HPC (SuperComputer) Environment Special IssueofI JCCT Vol. 2 Issue 2, 3, 4; 2010 for International Conference [ICCT-2010], 3rd-5th December 2010

3. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – [Электронный ресурс] – Режим доступа: http://docs.cntd.ru/document/gost-28147-89 (дата обращения 15.07.2020).

4. Цебренко К.Н. Концепция радиотелефонной связи на основе радиоудлинителя телефонной линии // Спецтехника и связь. – 2013. – №2. – С. 57-59.

5. Цебренко К.Н. Концепция разработки малой системы абонентского доступа к телефонной линии // Международный журнал гуманитарных и естественных наук. – 2019. – №8-2. – С. 43-54.

ANALYSIS OF ISSUES OF SECURITY OF INFORMATION SYSTEMS ON THE BASIS OF APPLICATION OF HIGH PERFORMANCE COMPUTER SYSTEMS

K.N. Tsebrenko, *Candidate of Technical Sciences, Associate Professor*
Academy of Marketing and Social Information Technologies – IMSIT
(Russia, Krasnodar)

Abstract. *An important issue of ensuring information security for high performance computing is the use of virtualization and cloud computing. This approach has created many new security risks that need to be investigated. The article considers the issue of using cryptographic protection methods to achieve data security in cloud systems based on the GOST 28147-89 algorithm. Issues related to data security and information about the HPC context during the organization of access to services and resources are investigated. The use and implementation of the GOST 28147-89 cryptographic algorithm is considered. Changes in the GOST 28147-89 algorithm are proposed: a random number generator is included to generate a key in the form of a random number. It is used as a key for encryption and decryption within one session. This method was tested when creating a prototype according to the proposed concept on the computing cluster of the Academy of Marketing and Social Information Technologies – IMSIT.*

Keywords: *analysis, security systems, encryption, high performance computing systems, generator, key.*