Программное обеспечение информационных и управляющих систем

А.В. Царегородцев
доктор техн. наук, профессор
E-mail: atsaregorodtsev@hse.ru
А.Б. Лось
канд. техн. наук, доцент
E-mail: alos@hse.ru
А.В. Сорокин
старший преподаватель
E-mail: asorokin@hse.ru
(ФГАОУ ВПО «Национальный исследовательский университет «Высшая школа экономики»)
Москва, Российская Федерация

Построение гибридной защищенной облачной среды ИТ-инфраструктуры организации

Облачные вычисления становятся одной из самых распространенных ИТ-технологий для развертывания приложений, благодаря своим ключевым особенностям: гибкости решения, доступности по запросу и хорошим соотношением цена/качество. Миграция на облачную архитектуру позволит организациям снизить общие затраты на внедрение и поддержку инфраструктуры и сократит время разработки новых бизнес-приложений. Однако наиболее острым и актуальным вопросом при миграции данных в облако является вопрос обеспечения информационной безопасности. Существует большое количество факторов, оказывающих влияние на комплексную безопасность облачной среды, так как ее многоарендная архитектура приносит новые и более сложные проблемы и уязвимости. В статье рассматриваются ключевые уровни построения облака, ряд существенных преимуществ и современных решений, которые получает организация при переходе на облачные технологии. Особое внимание уделено открытым вопросам информационной безопасности и вариантам их решения при построении комплексной системы защиты информации на облачной архитектуре.

Предложены различные варианты архитектуры гибридной защищенной облачной среды, которые позволят преодолеть существенные ограничения на уровне сервера базы данных и в то же время обеспечить необходимый уровень защищенности обрабатываемых данных. Применение рассмотренных ИТ-инфраструктур позволит организации обеспечить оптимальное использование ресурсов и существенно сократить время вычисления.

Ключевые слова: *облачные вычисления; угрозы информационной безопасности; облачные сервисы; гибридное облако; методы управления информационной безопасностью; требования информационной безопасности.*

A.V. Tsaregorodtsev
Doctor of Techn. Sciences, Professor
E-mail: atsaregorodtsev@hse.ru
A.B. Los
Cand. of Techn. Sciences, Associate Professor
E-mail: alos@hse.ru
A.V. Sorokin
Senior Lecturer
E-mail: asorokin@hse.ru
(Federal State Autonomous Educational Institution of Higher Professional Education «National Research University «Higher School of Economics»)
Moscow, Russian Federation

Development of Protected Hybrid Cloud Environment of Organizations IT-infrastructure

Cloud computing is becoming one of the most common IT technologies for deploying applications, thanks to its key features: flexible solutions, available on request, and a good price / performance ratio. Migrating to the cloud-based architecture allows organizations to reduce the total cost of implementation and support infrastructure, and reduce development time for new business applications. However, the most urgent and important point of migrating data to the cloud is the problem of information security. There are many factors that affect the security of a comprehensive cloud as it multirental architecture brings new and more complex problems and vulnerabilities. This article discusses the key levels of clouds design, some significant advantages and advanced solutions that organization receives during the transition to the cloud. Particular attention is paid to problems of information security and options for solutions in developing of integrated system of information security in the cloud architecture.

Different variants of the hybrid architecture of secure cloud that will overcome significant limitations on the level of the database server and at the same time ensure the necessary level of security of the processed data are offered. Applications discussed IT-infrastructures will enable to organization to ensure optimal use of resources and significantly reduce the computation time.

Keywords: *cloud computing; information security threats; cloud services; hybrid cloud; information security management methods; information security requirements.*

www.tgizd.ru

Введение

Достижение цели информационной безопасности организации становится одним из ключевых факторов для принятия решений об услугах аутсорсинга информационных технологий и, в частности, для принятия решения о миграции организационных данных, приложений и других ресурсов на инфраструктуру, основанную на среде облачных вычислений, как отмечается в авторской работе [1], согласно определению Национального института стандартов и технологий США [2].

Провайдеры, предоставляющие общедоступные облачные сервисы, как правило, не имеют четкого представления о требованиях безопасности конкретной организации. В связи с этим организации должны иметь возможность использовать систему управления информационной безопасности для облачных приложений и сервисов, соизмеримую или превосходящую ту, которая используется для систем, развернутых в рамках традиционной ИТ-модели, что показано в авторской работе [3].

Информационная безопасность облачной среды [4], имеет прямую зависимость от индивидуальной безопасности каждого компонента архитектуры: сервиса, системы самообслуживания, системы управления квотами на ресурсы, гипервизора (программы управления операционными системами), системы управления гостевыми виртуальными машинами, промежуточного программного обеспечения и системы хранения данных.

Мониторинг, решение проблем и контроль безопасности являются критически важными процессами в организации наряду с производительностью и доступностью. В связи с тем, что облачные вычисления несут с собой новые вызовы в области информационной безопасности, для организации крайне важно контролировать процесс управления информационной безопасностью облачной инфраструктуры. Уровень доверия к предоставляемым сервисам может значительно меняться в зависимости от целей организации, структуры ее активов, открытости для общественности, угроз, которым подвергается организация, а также приемлемого уровня информационного риска [5].

Анализ основных преимуществ использования облачных сред в качестве основы для построения информационно-телекоммуникационных сред, проведенный в авторской работе [3], показывает, что, несмотря на все преимущества, предоставляемые облачными решениями, такие как высокая масштабируемость, эластичность, учет потребления и самообслуживание по требованию, остаются нерешенными задачи обеспечения информационной безопасности таких систем.

В связи с этим возникает необходимость в разработке системного подхода к построению различных вариантов развертывания гибридной облачной среды с целью оптимизации использования ресурсов, повышения уровня защищенности критичных данных и сокращения времени вычисления.

Преимущества гибридной защищенной облачной среды ИТ-инфраструктуры организации

Как отмечается в работе [6], облачно-ориентированная бизнес-архитектура открывает новые преимущества для организаций, поэтому применение построения в ИТ-инфраструктуре организации именно облачной среды представляется вполне закономерным решением. Также, согласно техническому отчету, опубликованному в университете Беркли [7], облачная архитектура имеет для организаций ряд преимуществ, среди которых отсутствие необходимости для пользователей в долгосрочном планировании использования ресурсов, возможность начала деятельности с небольшим объемом ресурсов и его последующим увеличением, а также – в случае использования ресурсов стороннего провайдера – возможность оплаты только фактически используемых ресурсов (вычислительных ресурсов – на основе фактического времени использования, а хранилищ данных – на основе фактически использованного дискового пространства).

При построении гибридной защищенной облачной ИТ-инфраструктуры организации в первую очередь необходимо обратить внимание на архитектуру распределенной базы данных. В качестве отправной точки для обоснования практического применения и экономической обоснованности использования гибридных облачных сред примем во внимание классическую многоуровневую архитектуру. Это позволит показать все преимущества различных вариантов развертывания гибридной защищенной облачной среды по сравнению с системой, имеющей в основе классическую многоуровневую архитектуру, отмеченные, например, в работе [8].

В настоящее время достаточно широкое применение имеет классическая трехзвенная архитектура, которая поддерживается крупными вендорами программного обеспечения (например, SAP). В классической архитектуре балансировка (выравнивание) нагрузки подразумевает распределение процесса выполнения заданий между несколькими серверами сети с целью оптимизации использования ресурсов и сокращения времени вычисления.

Классическая архитектура (рис. 1) обладает рядом преимуществ, которые можно описать в виде следующих положений:

- использование лучших в своем классе компонентов на всех уровнях архитектуры;
- масштабирование и эластичность на уровне веб-приложений и уровне хранения данных.

Если пропускную способность бизнес приложений необходимо увеличить в связи с увеличением запросов со стороны конечных пользователей, происходит включение дополнительных аппаратных

www.tgzd.ru

мощностей на уровне сервера приложений. В случае падения нагрузки, дополнительные мощности могут быть оперативно выключены. На уровне хранения информации могут быть добавлены или удалены дополнительные накопители данных при увеличении нагрузки на систему, которая влияет на размер базы данных.

Потенциально узким местом классической архитектуры является сервер базы данных. Если сервер базы данных перегружен, то единственным решением будет являться покупка дополнительных аппаратных мощностей. Физические машины, которые используются в качестве серверов базы данных, как правило, являются очень дорогими в обслуживании, и используются только в пиковые нагрузки.

Таким образом, классическая трехуровневая архитектура имеет два существенных недостатка, заключающиеся в ограниченной масштабируемости и высокой стоимости владения, которые в свою очередь могут быть устранены с помощью предлагаемого подхода.

Рассмотрим различные варианты архитектуры гибридной защищенной облачной среды, которые позволят преодолеть эти существенные ограничения на уровне сервера базы данных и в то же время обеспечить необходимый уровень защищенности обрабатываемых данных. На рисунке 2 показан первый вариант построения гибридной облачной архитектуры.

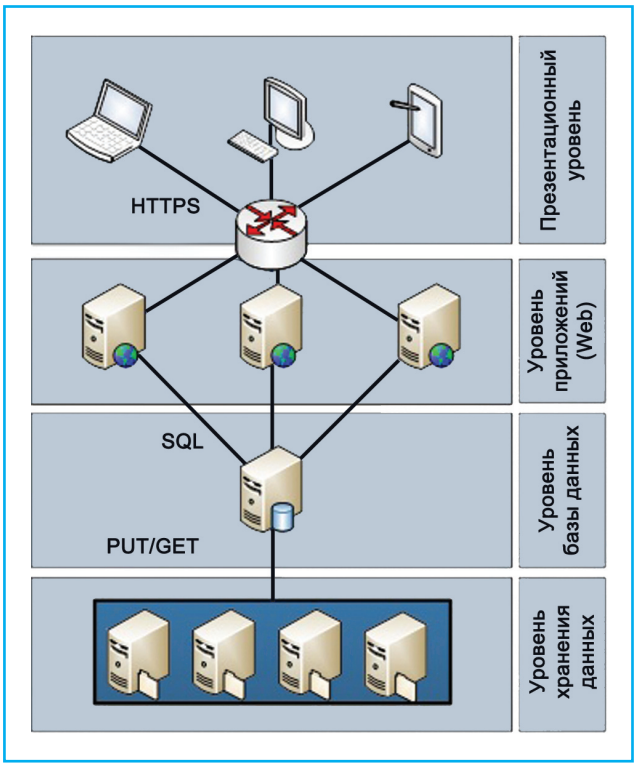

Рис. 1. Классический подход к построению трехзвенной архитектуры

В рамках этой архитектуры серверы базы данных могут размещаться на дешевых аппаратных машинах, которые будут оперировать с небольшой выборкой данных и поддерживать требуемый уровень нагрузки. Однако такое решение имеет ограничения при масштабировании, связанные с колебанием нагрузки: добавление или удаление аппаратных машин для поддержки высокой (или низкой) загруженности включает в себя распределение данных и их перемещение между машинами.

Для достижения хорошей масштабируемости и отказоустойчивости предлагается второй вариант построения гибридной облачной архитектуры.

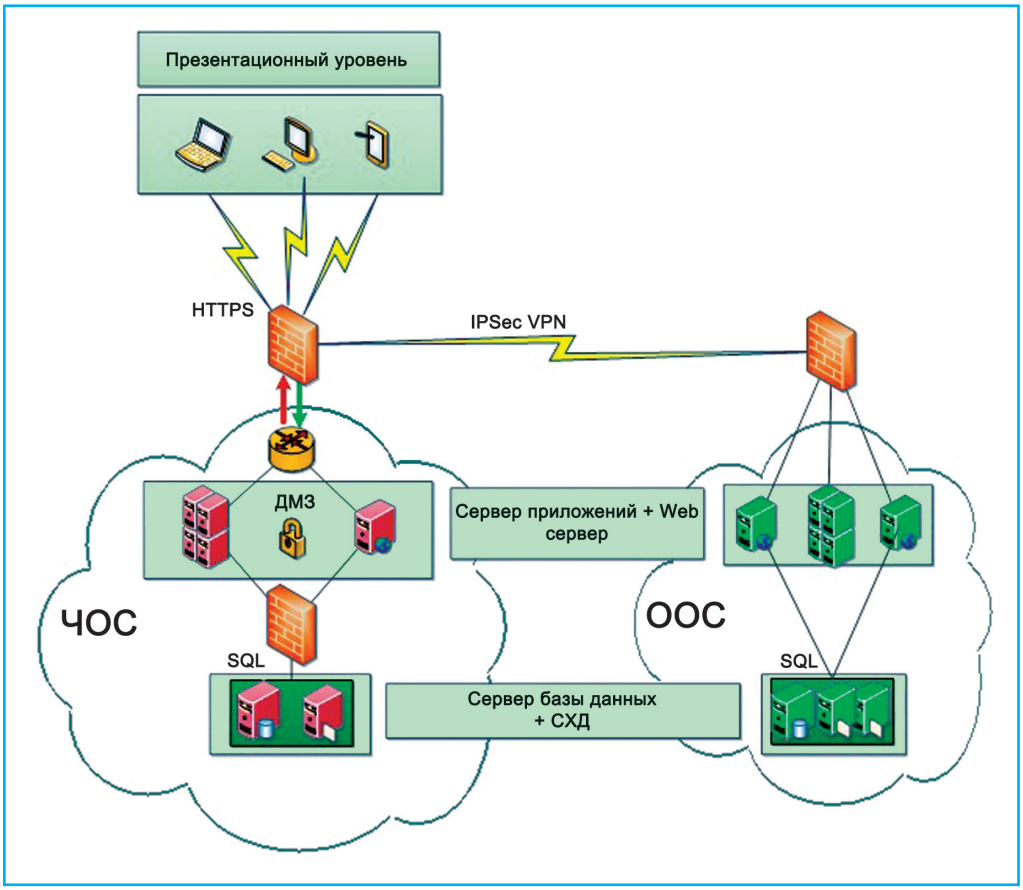

Рис. 2. Первый вариант верхнеуровневой архитектуры гибридной защищенной облачной среды

www.tgizd.ru

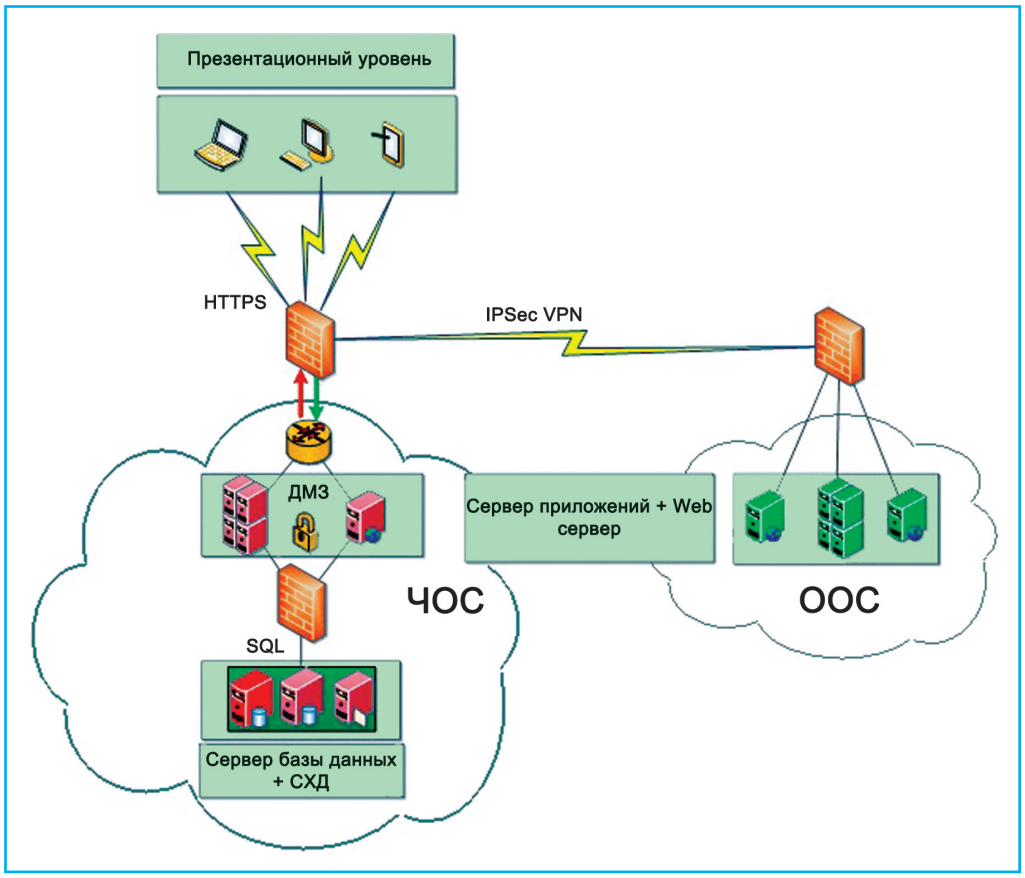

Рис. 3. Второй вариант верхнеуровневой архитектуры гибридной защищенной облачной среды

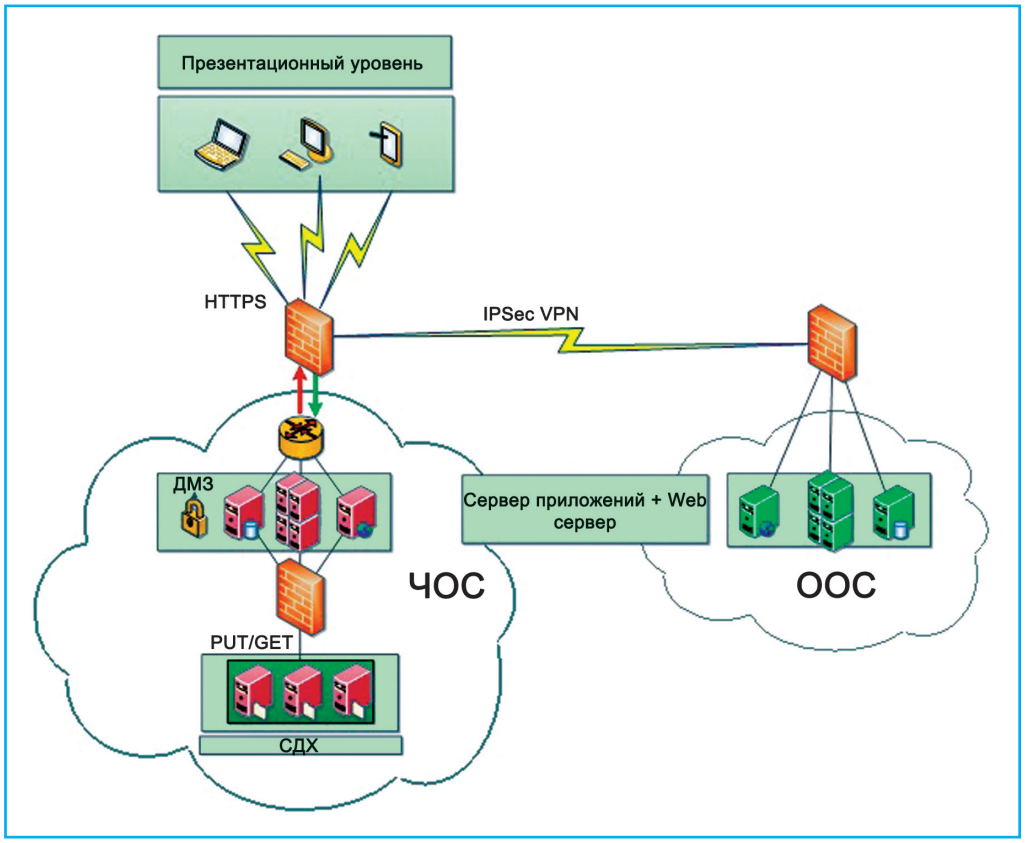

Рис. 4. Третий вариант верхнеуровневой архитектуры гибридной защищенной облачной среды

Здесь также используется несколько серверов базы данных (рис. 3). Каждый сервер базы данных управляет копией всей базы данных (или логического раздела базы данных). Наиболее важным аспектом такого варианта построения гибридной облачной архитектуры является достижение свойства консистентности данных. Если репликация не является прозрачной, то приложение направляет все запросы на обновление к серверу базы данных, который контролирует мастер-копию и мастер-сервер распространяет все успешно совершенные изменения на сервер-сателлиты. Приложения могут создавать запросы на чтение данных к любому серверу базы данных (мастер или сателлит). Если репликация прозрачна, то запросы автоматически направляются к мастер-серверу или его сателлиту (мастер-сервер отмечен красным цветом на рисунке 3).

В данном случае для поддержки серверов баз данных может быть использовано недорогое серийное аппаратное обеспечение для сервер-сателлитов. В то же время архитектура на рисунке 3 может быть масштабируема и сокращена в зависимости от рабочей нагрузки, если, например, совершаются только операции чтения. В любой момент времени сервер-сателлит может быть удален в связи с уменьшением нагрузки или добавлен при необходимости

www.tgizd.ru

проведения копирования данных из мастер-сервера на новый сервер.

Второй вариант построения гибридной архитектуры может предоставить хорошие возможности для увеличения масштабирования и надежности системы.

На рисунке 4 изображена архитектура, в рамках которой база данных представлена в виде распределенной системы.

Основное отличие от архитектуры, построенной во втором подходе, заключается в возможности использования диска коллективного пользования со слабыми связями между узлами для достижения хорошей масштабируемости. В данной архитектуре система хранения данных отделена от сервера базы данных и предусмотрен автономный и одновременный доступ к общим данным. Для того чтобы обеспечить синхронизированное чтение и запись к общим данным, необходимо использовать распределенные протоколы, которые обеспечивают согласованность данных на всех уровнях архитектуры. В целях сокращения расходов уровень базы данных объединен с уровнем веб-сервера и сервера приложений, таким образом, доступ к базе данных обеспечивается специальными библиотеками на уровне сервера приложений, а не отдельными процессами по работе с базой данных.

Данный вид архитектуры является наиболее подходящим для гибридной защищенной облачной среды, так как обеспечивает полную масштабируемость и эластичность на всех уровнях архитектуры. Каждый HTTPS-запрос может быть направлен напрямую на любой уровень архитектуры (веб-сервер, сервер приложений, сервер БД), что обеспечит полную масштабируемость. Кроме того, данные могут быть реплицированы и логически разделены на уровне хранилища данных, что может обеспечить улучшенную масштабируемость. Другим важным преимуществом распределенной архитектуры является возможность использования недорогих аппаратных машин на всех уровнях. Но такая масштабируемость имеет свою цену. Так как согласно теореме CAP (теореме Брюера), в распределенной системе невозможно обеспечивать одновременное выполнение всех трех условий: корректности, доступности и устойчивости к сбоям узлов. *Amazon S3* поддерживает распределенную архитектуру, в рамках которой достигается только свойство «возможной корректности». Согласованность в конечном счете (*eventual consistency*) представляет собой частный случай «слабой согласованности». Система гарантирует, что, при отсутствии новых обновлений данных, в конечном счете, все запросы будут возвращать последнее обновленное значение. При отсутствии сбоев максимальный размер окна несогласованности может быть определен на основании таких факторов, как задержка связи, загруженность системы и количество реплик в соответствии со схемой репликации.

Заключение

Одной из ключевых особенностей облачных систем является возможность удаленного доступа к предоставляемым сервисам. Но помимо очевидных преимуществ такого подхода возникает вопрос о хранении критичных данных. Обеспечение безопасности облачных систем широко обсуждается в профессиональном сообществе, например в работах [9…11], но до единого структурированного мнения пока далеко. В статье предложена принципиально новая концепция, которая лучше соответствуют духу облачных систем, чем традиционный подход. Еще одним важным фактором развития облачных технологий является создание защищенных облачных систем. Преимущества, предоставляемые облачными средами, постепенно осознаются рынком, но вместе с тем нельзя не признать, что существует множество как технических, так и организационных проблем. Зачастую это вынуждает бизнес переоценивать риски и действовать крайне аккуратно. На сегодняшний день использование облаков (как частных, так и публичных) должно опираться на ряд компромиссов, которые позволяют получить наибольшую выгоду при минимальных рисках, но готовых методологий построения подобных решений пока не представлено. В статье предложены возможные пути к решению этих проблем.

Список литературы

1. Царегородцев А.В., Качко А.К., Лавриненко М.М. Один из подходов к построению гибридной защищенной облачной среды // *Безопасность информационных технологий*. 2014. № 1. С. 22–28.
2. Mell P., Tim Grance T. The NIST Definition of Cloud Computing, Version 15, September, 2011. URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
3. Царегородцев А.В., Качко А.К. Один из подходов к управлению информационной безопасностью при разработке информационной инфраструктуры организации // *Национальная безопасность*. 2012. № 1 (18). С. 46–59.
4. Царегородцев А.В., Качко А.К. Обеспечение информационной безопасности на облачной архитектуре организации // *Национальная безопасность*. 2011. № 5. С. 25–34.
5. Царегородцев А.В., Макаренко Е.В. Оптимизация архитектуры гибридной среды облачных вычислений по критерию совокупной стоимости владения // *Безопасность информационных технологий*. 2014. № 4. С. 59–68
6. *Fingar P.* Extreme Competition: Cloud Oriented Business Architecture. Business Process Trends (2009).
7. Waxer C. (2010). The benefits of cloud computing. Webhostingunleashed.com. URL: http://www.webhostingunleashed.com/features/cloud-computing-benefits/ (дата обращения: 12.09.15).
8. Armbrust M., Fox A., Griffith R., Joseph A.D., Katz R.H., Konwinski A., Lee G., Patterson D.A., Rabkin A., Stoica I., Zaharia M.: Above the clouds: a Berkeley view of cloud computing. Technical Report No. UCB/EECS-2009-28, Electrical

www.tgizd.ru

Engineering and Computer Sciences, University of California at Berkeley (2009).
9. Cloud Security Alliance (2010). Top Threats to Cloud Computing. Cloud Security Alliance. URL: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (дата обращения: 12.09.15).
10. Chen D.W., He Y.J. A Study on Secure Data Storage Strategy in Cloud Computing, Journal of Convergence Information Technology, AICIT, Vol. 5, No. 7, pp. 175–179, 2010.
11. Cloud Security Alliance, December 2009. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. URL: http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf (дата обращения: 12.09.15).

References

1. Tsaregorodtsev A.V., Kachko A.K., Lavrinenko M.M. Odin iz podkhodov k postroeniyu gibridnoy zashchishchennoy oblachnoy sredy [One approach to building a secure hybrid cloud]. *Bezopasnost informatsionnykh tekhnologiy* [Safety of information technology]. 2014, no. 1, pp. 22–28.
2. Mell P., Tim Grance T. The NIST Definition of Cloud Computing, Version 15, September, 2011. URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
3. Tsaregorodtsev A.V., Kachko A.K. Odin iz podkhodov k upravleniyu informatsionnoy bezopasnostyu pri razrabotke informatsionnoy infrastruktury organizatsii [One of the approaches to the management of information security in the development of information infrastructure]. *Natsionalnaya bezopasnost* [National Security]. 2012, no. 1 (18), pp. 46–59.
4. Tsaregorodtsev A.V., Kachko A.K. Obespechenie informatsionnoy bezopasnosti na oblachnoy arkhitekture organizatsii [Ensuring information security in cloud architecture organization]. *Natsionalnaya bezopasnost* [National Security]. 2011, no. 5, pp. 25–34.
5. Tsaregorodtsev A.V., Makarenko E.V. Optimizatsiya arkhitektury gibridnoy sredy oblachnykh vychisleniy po kriteriyu sovokupnoy stoimosti vladeniya. [Optimization of the architecture of the hybrid cloud environment criterion TCO]. *Bezopasnost informatsionnykh tekhnologiy* [Safety of information technology]. 2014, no. 4, pp. 59–68.
6. Fingar P. Extreme Competition: Cloud Oriented Business Architecture. Business Process Trends (2009).
7. Waxer C. (2010). The benefits of cloud computing. Webhostingunleashed.com. URL: http://www.webhostingunleashed.com/features/cloud-computing-benefits/ (12.09.15).
8. Armbrust M., Fox A., Griffith R., Joseph A.D., Katz R.H., Konwinski A., Lee G., Patterson D.A., Rabkin A., Stoica I., Zaharia M.: Above the clouds: a Berkeley view of cloud computing. Technical Report No. UCB/EECS-2009-28, Electrical Engineering and Computer Sciences, University of California at Berkeley (2009).
9. Cloud Security Alliance (2010). Top Threats to Cloud Computing. Cloud Security Alliance. URL: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (12.09.15)
10. Chen D. W., He Y. J. A Study on Secure Data Storage Strategy in Cloud Computing, Journal of Convergence Information Technology, AICIT, Vol. 5, No. 7, pp. 175–179, 2010.
11. Cloud Security Alliance, December 2009. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. URL: http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf (12.09.15).

Информация об авторах

Царегородцев Анатолий Валерьевич, доктор техн. наук, профессор Кафедры компьютерной безопасности
E-mail: atsaregorodtsev@hse.ru
Лось Алексей Борисович, канд. техн. наук, доцент, заведующий Кафедрой компьютерной безопасности, академический руководитель образовательной программы «Компьютерная безопасность»
E-mail: alos@hse.ru
Сорокин Александр Владимирович, старший преподаватель, заместитель заведующего Кафедры компьютерной безопасности
E-mail: asorokin@hse.ru
Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Национальный исследовательский университет «Высшая школа экономики»
123458, Российская Федерация, Москва, ул. Таллинская, д. 34

Information about the authors

Tsaregorodtsev Anatoly Valerevich, Doctor of Techn. Sciences, Professor of Departament of Computer Security
E-mail: atsaregorodtsev@hse.ru
Los Aleksey Borisovich, Cand. of Techn. Sciences, Associate Professor, Head of the Department of Computer Security, the academic director of the educational program «Computer Security»
E-mail: alos@hse.ru
Sorokin Aleksandr Vladimirovich, Senior Lecturer, Deputy Head of Department of Computer Security
E-mail: asorokin@hse.ru
Federal State Autonomous Educational Institution of Higher Professional Education «National Research University «Higher School of Economics»
123458, Russian Federation, Moscow, Str. Tallinn, 34