§3 ТЕХНОЛОГИИ И МЕТОДОЛОГИЯ В СИСТЕМАХ БЕЗОПАСНОСТИ

Лось А.Б., Царегородцев А.В., Сорокин А.В.

КОМПЛЕКСНЫЙ ПОДХОД К ПОСТРОЕНИЮ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА БАЗЕ ГИБРИДНОЙ ОБЛАЧНОЙ СРЕДЫ

Аннотация. *В статье рассматриваются вопросы обеспечения информационной безопасности в сфере облачных технологий. Информационно – телекоммуникационные системы, функционирующие на основе технологии облачных вычислений, в последнее время получают все большее распространение в связи с постоянно растущими потребностями в работе с большими объемами данных. При этом ключевым моментом в использовании облачных технологий является вопрос обеспечения надежной защиты данных при их передаче, обработке и хранении. В статье указаны основные проблемы применения облачных вычислений с точки зрения обеспечения информационной безопасности и рассматриваются варианты их решения при построении комплексной системы защиты информации на облачной архитектуре. Для решения поставленной задачи применяется метод теоретического анализа исходных данных в различных областях рассматриваемого вопроса, метод обобщения полученных результатов и выработки необходимых путей решения. Научная новизна работы состоит в проведении теоретического анализа всех сторон данной проблемы, включающего исследование угроз информации в облачной сфере, существующих решений в указанном направлении и разработке на основе полученных результатов процедуры комплексной защиты облачных вычислений. Предложены варианты применения облачных технологий для обработки и хранения информации различных категорий, в том числе, и критичных активов. Для работы с такими данными предлагается создавать гибридную облачную среду, предусматривающую включение в традиционную облачную архитектуру элементы частных облаков.*

Ключевые слова: *информационно-телекоммуникационные системы, облачные вычисления, гибридная облачная среда,, частные облака, критичные архивы, угрозы информационной безопасности,*

DOI: 10.7256/2073-8560.2016.3.16542

управление информационной безопасностью, требования информационной безопасности, информационные активы, информационные риски.

Abstract. *This article examines the issues of ensuring information security in the sphere of cloud technologies. Information and telecommunication systems, operating on the basis of cloud computing technology, over the recent years have become more widespread, with constantly growing needs in processing of the large volumes of data.The key point in the use of cloud computing is the issue of ensuring reliable protection of data during transmission, processing and storage. The article identifies the main problems of cloud computing from the point of view of information security and examines solutions when building complex systems of information protection in cloud architecture. In order too solve this issue, this work applies the method of theoretical analysis of the source data in various areas of the matter under consideration, the method of summarizing the results and formulating appropriate solutions. Scientific novelty of the work consists in a theoretical comprehensive analysis of this problem, including examination of threat to information in the cloud field, existing solutions in the specified direction and development on the basis of the results of the procedure for the comprehensive protection of cloud computing. Proposed applications of cloud computing for processing and storage of information of various categories, including critical assets. For working with such data, it is proposed to create a hybrid cloud environment, incorporating traditional cloud architecture elements of private clouds.*
Key words: *information risks, security requirements, information assets, information security management, information security threats, critical archives, private cloud, hybrid cloud, cloud computing, information and telecommunication systems.*

Введение

Среди приоритетных проблем научных исследований в области обеспечения информационной безопасности, утвержденных Научным советом при Совете Безопасности Российской Федерации, особую актуальность имеют следующие научно-технические проблемы.

1. Исследование проблем выбора архитектуры и расчета параметров защищенных информационно-телекоммуникационных систем, математических моделей и технологий управления, системного и прикладного программного обеспечения с интеграцией функций защиты, средств взаимодействия, устройств передачи и распределения информации.

Современный уровень развития информационно-телекоммуникационных технологий делает доступными новые варианты развёртывания ИТ-инфраструктуры организации, функционирующей в среде облачных вычислений. Облачные вычисления являются одной из самых привлекательных информационных технологий, предоставляющих многочисленные преимущества, среди которых в первую очередь можно выделить хорошую масштабируемость, доступность по запросу, возможность обработки распределенной информации. Кроме того, применение облачных сервисов позволяет обеспечить гибкость и свободный выбор необходимых вычислительных мощностей, в том числе и с учетом сезонных потребностей. Такой подход позволяет компаниям значительно расширить свою инфраструктуру, добавляя по мере надобности необходимую вычислительную емкость. Отличительной особенностью облачных вычислений является быстрое предоставление услуг и доступ к ресурсам в любом месте и в любое время.

2. Исследование проблем управления распределенными вычислительными процессами.

Виртуализация отличается возможностью оперативного и гибкого перераспределения ИТ-ресурсов между потребителями и очевидной экономией на масштабе, что и определяет неизбежность доминирования этого сервиса в корпоративных решениях. Последующее развитие ИТ показало, что логическими следствиями виртуализации являются аутсорсинг ИТ-сервисов и облачные вычисления, которые выступают как потенциальные мультипликаторы эффективности, достигнутой благодаря сервисам виртуализации. Предварительные оценки экономии на облачных решениях свидетельствуют о возможности сокращения посредством «облаков» затрат на эксплуатацию ИТ в среднем на 60-70%. Подобная экономия открывает возможность переключения высвобождаемых заметных фи-

DOI: 10.7256/2073-8560.2016.3.16542

нансовых и кадровых ресурсов на решение новых задач и соответствующую модернизацию экономик.

Но облачные вычисления наряду с очевидными преимуществами несут дополнительные риски и проблемы. И в первую очередь – это проблемы информационной безопасности при хранении, обработке и передаче данных. Проблемы информационной безопасности при применении облачных вычислений рассматриваются во многих публикациях (см., например, [1-6]). В частности, в статье [6] отмечен тот факт, что в отличие от традиционных центров обработки данных, где доступ персонала к серверам строго контролируется на физическом уровне, в облачных вычислениях доступ персонала происходит через Интернет, что приводит к появлению соответствующих многочисленных угроз. Следует отметить влияние на безопасность облачных сред и некоторых особенностей виртуальных машин. Виртуальные машины могут быть легко приостановлены, перезапущены, а также оперативно возвращены в предыдущее состояние. Кроме этого, они могут быть клонированы, а также перемещены между физическими серверами. Подобная изменчивость виртуальных машин существенно усложняет создание и поддержание целостной системы безопасности. Уязвимости и ошибки в настройках могут бесконтрольно распространяться. Кроме этого, достаточно сложно зафиксировать для последующего аудита состояние защиты в определенный момент времени, как отдельной виртуальной машины, так и системы в целом. Поскольку серверы облачных вычислений используют те же операционные системы и те же приложения, что обычные сервера, то для них угроза несанкционированного доступа или заражения так же высока. Кроме того, организация параллельной работы множества виртуальных машин существенно увеличивает атакуемую поверхность и повышает риск проведения успешной атаки.

При использовании облачных вычислений исчезает такое понятие, как периметр корпоративной сети, при этом общий уровень защищенности определяется уровнем наименее защищенной составляющей сети. Корпоративный межсетевой экран, основной компонент для внедрения политик безопасности и разграничения сегментов сети, не в состоянии повлиять на серверы, размещенные в облачных средах и на доступ к тем или иным ресурсам – теперь это ответственность провайдера облачных вычислений.

Метод построения системы защиты информации на облачной архитектуре

Открытые вопросы информационной безопасности не позволяют построить защищенные облачные сервисы для обработки критичных активов. Только включение в архитектуру демилитаризованных зон (ДМЗ) в виде частной облачной среды (ЧОС) может позволить обеспечить требуемый уровень безопасности обрабатываемых данных.

Для частной облачной среды характеры преимущества традиционной (внутренней) ИТ-инфраструктуры, а именно: возможность применения лучших практик, методик и метрик для анализа и оценки рисков, полный контроль всех ключевых процессов управления ИБ с возможностью проведения внутреннего аудита. Кроме того, сервисы на базе частных облаков способны предложить поставщику и конечному пользователю более высокую степень контроля, в том числе, доступ пользователей к сети, что существенно повышает безопасность информационной системы и ее устойчивость.

Основной проблемой применения ЧОС являются серьёзные финансовые издержки при их разработке и эксплуатации, ограниченная масштабируемость, отказоустойчивость и в дополнение ко всем угрозам, характерным для общедоступной среды, можно отнести ошибки стратегического планирования использования вычислительных мощностей, которые могут привести к снижению доступности, целостности и защищенности обрабатываемых данных.

Включение ДМЗ зон в облачную архитектуру необходимо, чтобы организация могла в полной мере обеспечить контроль над критичными активами, даже, несмотря на большие финансовые издержки при его эксплуатации. Общественное облако необходимо для предоставления требуемого уровня масштабируемости и гибкости в выделении ресурсов по требованию в моменты пиковых нагрузок на систему.

Использование компонентов с разным уровнем безопасности приводит к появлению нового, гибридного типа развертывания облачной среды.

В настоящей заметке, для построения защищенной облачной инфраструктуры организации, предлагается метод реализации гибридной защищенной облачной среды (ГЗОС). Применение данного метода позволит обеспечить

DOI: 10.7256/2073-8560.2016.3.16542

выполнение требований безопасности, определить последовательность обработки критичных данных, обеспечить расположение этих данных между защищенными компонентами облачной среды. Основываясь на приведенных выше ключевых этапах анализа информационной безопасности облачной инфраструктуры, опишем метод в нотации EPC (Event-Driven Process Chain, событийная цепочка процессов).

Этап 1. Идентификация и оценка критичных активов организации – рисунок 1.

После принятия решения о миграции данных в облачную среду специалист бизнес подразделения проводит анализ информационных активов, участвующих в бизнес процессах, которые, в свою очередь, планируется автоматизировать в рамках облачной среды. Для этого он детализирует и подробно описывает бизнес процесс организации с обязательным указанием моментов, связанных с обработкой критичных данных. Данные о возможном финансовом ущербе, который может понести компания в случае несанкционированного доступа к конфиденциальной информации должны учитываться при построении и выборе облачной архитектуры.

Этап 2. Идентификация требований безопасности и определение последовательности обработки данных в ГЗОС – рисунок 2.

Сотрудник службы информационной безопасности (ИБ) проводит анализ требований безопасности ИТ системы, построенной на технологии облачных вычислений. Далее формируется условия безопасного функционирования рабочего процесса и выбирается подходящий вариант гибридной защищенной облачной среды (ГЗОС). Затем определяются основные компоненты ГЗОС и варианты распределения ее процессов. Один из подходов к построению деревьев целей ИБ облачной инфраструктуры организации рассмотрен в работе [8]. Критериально-математический аппарат «измерения» свойства системности на деревьях целей на основе таких алгебраических объектов, как полугруппы с единицей – моноидов, подробно рассмотрен в работе [9].

Последовательность обработки критичных данных на базе формализованной модели безопасности процесса обработки данных в условиях среды облачных вычислений детально рассмотрена в работе [10].

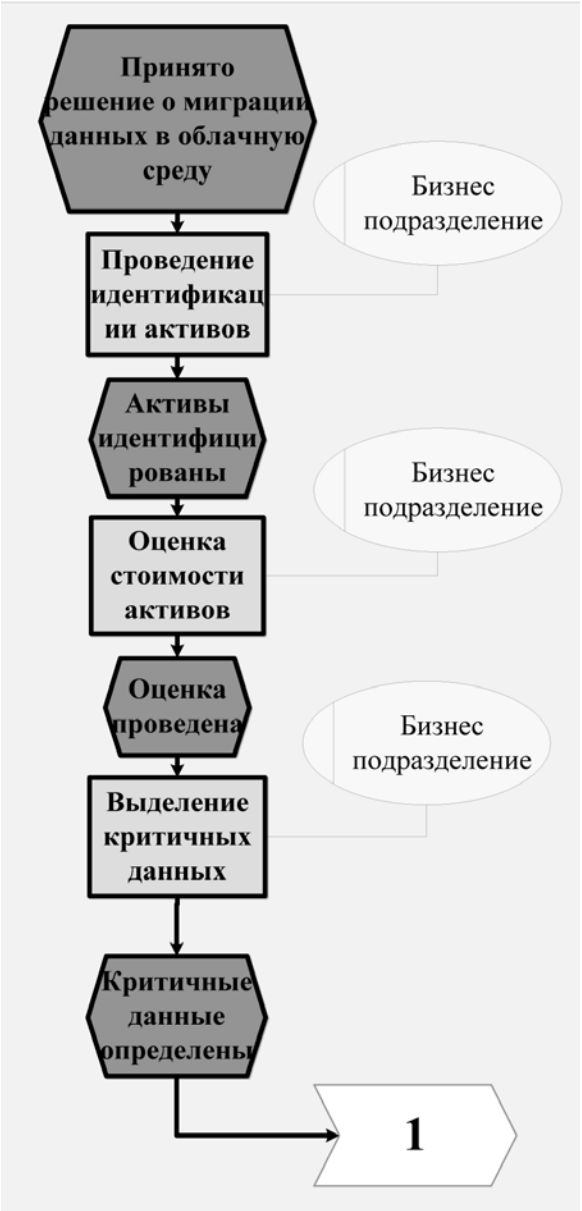

Рис. 1. Идентификация и оценка критичных активов организации

Этап 3. Идентификация угроз и построение риск модели ГЗОС – рисунок 3.

Управление информационными рисками является центральным процессом в вопросах обеспечения информационной безопасности.

Для каждого информационного актива, необходимо определить уровень его уязвимости, наличие потенциальных угроз, способных использовать эти уязвимости, а также оценить влияние инцидентов безопасности на бизнес процессы организации в рамках повседневной работы. Важным моментом построения риск – модели ГЗОС является определение величины приемлемого риска и процедуры его пересмотра. Чтобы успешно реализовать все действия процесса ана-

DOI: 10.7256/2073-8560.2016.3.16542

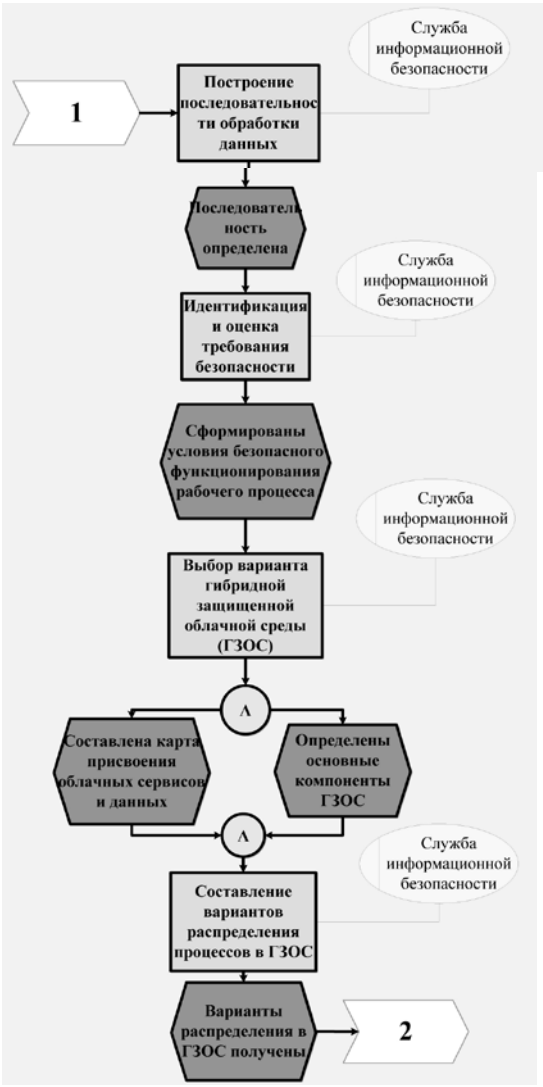

Рис. 2. Идентификация требований безопасности и определение последовательности обработки данных в ГЗОС

лиза риска необходимо внедрить в организации процессы контроля и применения контрмер.

Этап 4. Применение стоимостной методики и построение архитектуры ГЗОС – рисунок 4**.**

Сотрудник службы ИБ на основании соответствующей методики определяет стоимость различных вариантов развёртывания ГЗОС, с учетом практических рекомендаций осуществляет выбор различных вариантов построения архитектуры ГЗОС и представляет их на рассмотрение и утверждение руководства организации. После рассмотрения представленных вариантов руководством организации и выбора наиболее подходящего осуществляется этап непосредственной реализации и эксплуатации ГЗОС.

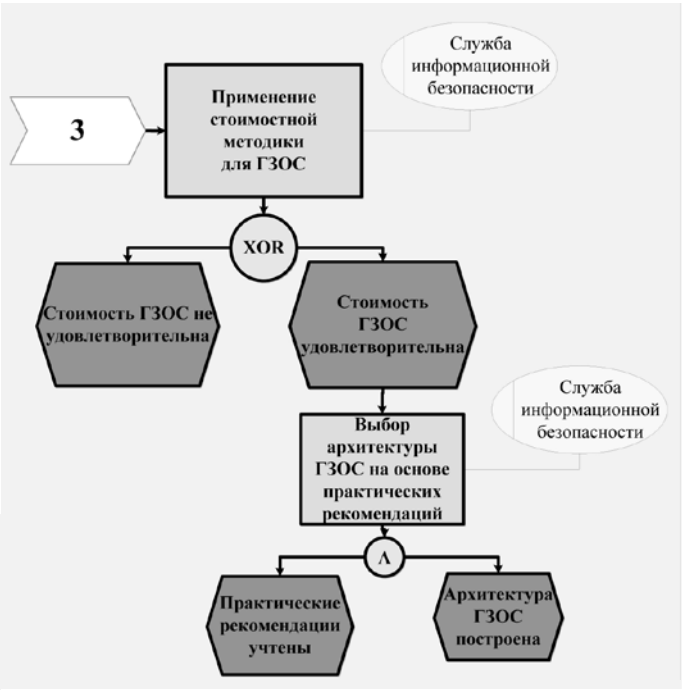

Рис. 4. Применение стоимостной методики и построение архитектуры ГЗОС

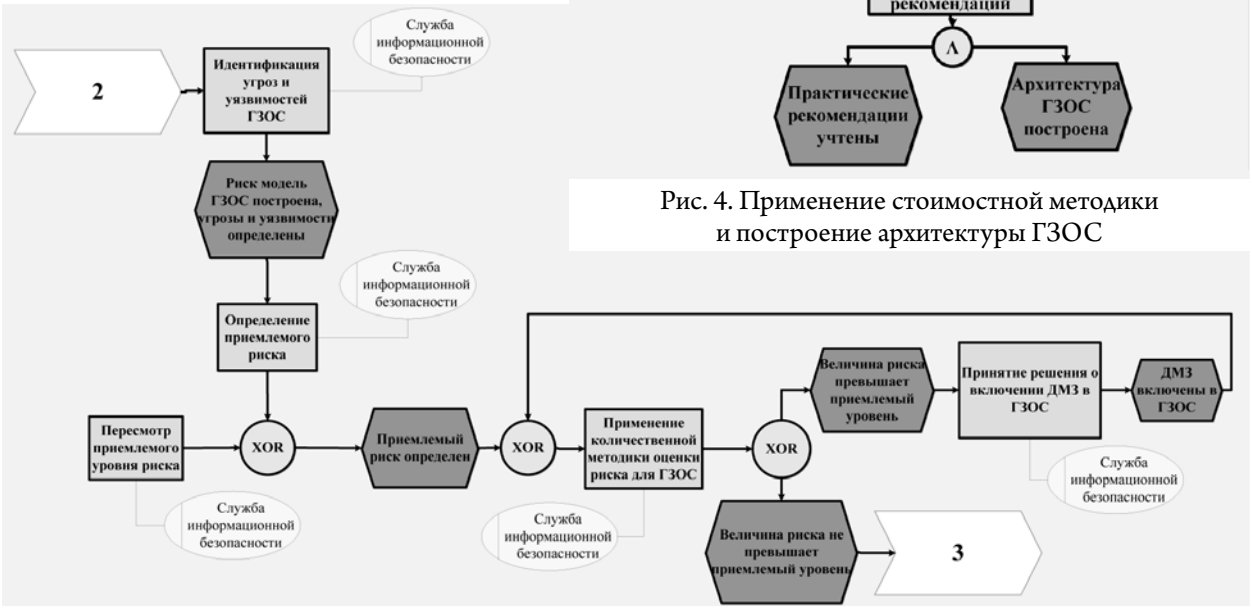

Рис. 3. Идентификация угроз и построение риск модели ГЗОС

DOI: 10.7256/2073-8560.2016.3.16542

Заключение

В настоящей работе для решения задачи формирования защищенной облачной инфраструктуры организации предложен метод построения гибридной защищенной облачной среды. Применение разработанного метода позволит существенно повысить эффективность использования ИТ-ресурсов, значительно сократить их стоимость за счет диверсификации информационных потоков организации при их миграции на гибридную облачную архитектуру, обеспечить выполнение требований безопасности, определить последовательность обработки критичных данных и обеспечить расположение этих данных между защищенными компонентами облачной среды.

БИБЛИОГРАФИЯ

1. Облачная безопасность – взгляд из Европы.–режим доступа: http://cloudzone.ru/ articles/ analytics/51.html.
2. Облачные сервисы. Взгляд из России/Под ред. Е. Гребнева.–М.: CNews.-2011.-34 с.
3. Сюртуков И.В. Что мешает активному переходу заказчиков в России к «облачным» технологиям? Портал iBusiness.–режим доступа: http://i-business.ru/blogs/11529 .
4. Сообщество Security Focus.–Режим доступа:http://www.security focus.com/tools/3189.
5. Thompson B. Storm warning for cloud computing.–режим доступа: http://www.news.bbc.co.uk/2/ hi/technology/7421099.stm.
6. Кабанов А.С., Лось А.Б. Вопросы обеспечения информационной безопасности при использовании облачных технологий в государственном секторе //Качество. Инновации. Образование. М.:«Известия».-2014.-№6(109).-С.33-39.
7. National Institute of Standards and Technology (NIST). Definition of .–режим доступа: Cloud Computing http://csrc.nist.gov/groups/SNS/cloud-computing/
8. Царегородцев А.В. Построение деревьев целей для идентификации требований безопасности среды облачных вычислений//Национальная безопасность.–М.: Изд-во «НБ Медиа».-2013.–№5(28).–С.51-69.
9. Царегородцев А.В., Кислицын А.С. Основы синтеза защищенных телекоммуникационных систем.– М.: Радиотехника.-2006.-244с.
10. Царегородцев А.В., Качко А.К. Один из подходов к управлению информационной безопасностью при разработке информационной инфраструктуры организации//Национальная безопасность.– М.: Изд-во «НБ Медиа».-2012.-№1(18).– С.46-59.

REFERENCES (TRANSLITERATED)

1. Oblachnaya bezopasnost' – vzglyad iz Evropy.–rezhim dostupa: http://cloudzone.ru/ articles/ analytics/51.html.
2. Oblachnye servisy. Vzglyad iz Rossii/Pod red. E. Grebneva.–M.: CNews.-2011.-34 s.
3. Syurtukov I.V. Chto meshaet aktivnomu perekhodu zakazchikov v Rossii k «oblachnym» tekhnologiyam? Portal iBusiness.–rezhim dostupa: http://i-business.ru/blogs/11529 .
4. Soobshchestvo Security Focus.–Rezhim dostupa:http://www.security focus.com/tools/3189.
5. Thompson B. Storm warning for cloud computing.–rezhim dostupa: http://www.news.bbc.co.uk/2/ hi/technology/7421099.stm.
6. Kabanov A.S., Los' A.B. Voprosy obespecheniya informatsionnoi bezopasnosti pri ispol'zovanii oblachnykh tekhnologii v gosudarstvennom sektore //Kachestvo. Innovatsii. Obrazovanie. M.:«Izvestiya».-2014.-№6(109).-S.33-39.
7. National Institute of Standards and Technology (NIST). Definition of .–rezhim dostupa: Cloud Computing http://csrc.nist.gov/groups/SNS/cloud-computing/
8. Tsaregorodtsev A.V. Postroenie derev'ev tselei dlya identifikatsii trebovanii bezopasnosti sredy oblachnykh vychislenii//Natsional'naya bezopasnost'.–M.: Izd-vo «NB Media».-2013.–№5(28).–S.51-69.
9. Tsaregorodtsev A.V., Kislitsyn A.S. Osnovy sinteza zashchishchennykh telekommunikatsionnykh sistem.– M.: Radiotekhnika.-2006.-244s.
10. Tsaregorodtsev A.V., Kachko A.K. Odin iz podkhodov k upravleniyu informatsionnoi bezopasnost'yu pri razrabotke informatsionnoi infrastruktury organizatsii//Natsional'naya bezopasnost'.–M.: Izd-vo «NB Media».-2012.-№1(18).– S.46-59.

DOI: 10.7256/2073-8560.2016.3.16542