РАЗРАБОТКА КОМПЛЕКСНОГО МЕТОДА ПОСТРОЕНИЯ ГИБРИДНОЙ ЗАЩИЩЕННОЙ ОБЛАЧНОЙ СРЕДЫ ОРГАНИЗАЦИИ

Качко Андрей Константинович,
аспирант, Всероссийская государственная налоговая академия Министерства финансов Российской Федерации,
05.13.19
akkachko@gmail.com

Аннотация. *Облачные вычисления в ближайшем будущем станут одной из самых распространенных ИТ технологий для развертывания приложений, благодаря своим ключевым особенностям: гибкости решения, доступности по запросу и хорошим соотношением цена/качество. Существует большое количество факторов, оказывающих влияние на комплексную безопасность облачной среды, так как её многоарендная архитектура приносит новые и более сложные проблемы и уязвимости. В статье особое внимание уделено открытым вопросам информационной безопасности и вариантам их решения при построении комплексной системы защиты информации на облачной архитектуре.*

Ключевые слова: облачные вычисления, общедоступная облачная среда, частная облачная среда, гибридная защищенная облачная среда, угрозы информационной безопасности, анализ информационных рисков, методы управления информационной безопасностью, бизнес активы, требования информационной безопасности.

APPLICATION OF THE COMPLEX METHOD FOR CREATION HYBRID CLOUD SECURE ENVIRONMENT

Kachko Andrei Konstantinovich
graduate student, All Russian State Tax Academy,

Abstract. *Cloud computing will be one of the most common IT technologies to deploy applications, due to its key features: on-demand network access to a shared pool of configurable computing resources, flexibility and good quality/price ratio. Migrating to cloud architecture enables organizations to reduce the overall cost of implementing and maintaining the infrastructure and reduce development time for new business applications. There are many factors that influence the complex security environment of cloud, as its multitenant architecture brings new and more complex problems and vulnerabilities are received by the organization during the transition to cloud technology. Particular attention in the paper is paid to the public on information security and ways of their solutions in the construction of an integrated information security management system on the cloud architecture.*

Keywords: cloud computing, public cloud, private cloud, secure hybrid cloud, information security threats, business assets, security requirements, classification of risk management methods.

Достижение целей информационной безопасности (ИБ) 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.

Провайдеры, предоставляющие общедоступные облачные сервисы, как правило, не имеют чёткого представления о требованиях безопасности конкретной организации. В связи с этим, организации должны иметь возможность использовать систему управления информационной безопасности (СУИБ) для облачных приложений и сервисов, соизмеримую или превосходящую ту, которая используется для систем, развёрнутых в рамках традиционной ИТ-модели.

Информационная безопасность облачной среды 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 [1].

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 её активов, открытости для публики, угроз, которым подвергается организация, а также приемлемого уровня информационного риска.

Управление информационными рисками, определение пригодности облачных сервисов для организации невозможно без понимания контекста, в котором работает организация и последствий от возможных видов угроз, с которыми она может столкнуться в результате своей деятельности. То, что хорошо работает для одной организации, не обязательно будет работать для другой, большинство организаций не могут себе позволить в финансовом отношении защитить все свои вычислительные ресурсы и активы, поэтому особое внимание должно уделяться вариантам обеспечения безопасности на основании соотнесения стоимости решения, а также критичности обрабатываемых данных.

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

Слабой стороной общедоступной среды облачных вычислений с точки зрения информационной безопасности является невозможность гибкого управления и контроля состояния информационной безопасности инфраструктуры со стороны клиента (организации). Приведем наиболее серьезные открытые вопросы безопасности общедоступной облачной среды.

- **Отсутствие контроля над состоянием аппаратной части.** Контроль над состоянием виртуальной части облачной инфраструктуры могут осуществлять только IaaS клиенты, в то время как PaaS и SaaS клиенты такой возможности не имеют.
- **Отсутствие подробного журнала.** Провайдеры общедоступных облачных сред не предоставляют возможность ведения детального журнала для анализа действий пользователей и администраторов системы, что может сильно усложнить расследование инцидентов информационной безопасности.
- **Трудности с доступом к доказательной базе**. Сохранение и выемка доказательной базы в случае незаконной деятельности клиента может быть затруднена в силу географического распределения данных в рамках инфраструктуры провайдера.
- **Отсутствие прозрачности работ провайдера.** С точки зрения клиента общедоступного облака набор предоставляемых услуг выглядит, как чёрный ящик без исходного кода используемых приложений. Это совершается с целью обеспечить конфиденциальность некоторых аспектов защиты облачных сервисов и предотвратить использование «узких мест» инфраструктуры провайдера.
- **Зависимость от канала связи.** Для эффективного использования облачных сервисов требуется наличие широкополосного доступа в Интернет. Отсутствие требуемой пропускной способности сети может сильно снизить время реакции системы на действия конечного пользователя.

Сложные процедуры миграции данных. Миграция данных (начальная загрузка) в публичную среду облачных вычислений или смена провайдера является серьёзной проблемой и требует больших финансовых и людских затрат со стороны клиента.

Приведенные 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 может позволить обеспечить требуемый уровень безопасности обрабатываемых данных.

Для частной облачной среды (ЧОС) 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. Основной проблемой являются серьёзные финансовые издержки при создании и эксплуатации ЧОС, 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.

Для решения задачи построения защищенной облачной инфраструктуры организации предлагается рассмотреть комплексный метод построения защищенной гибридной облачной среды (ГЗОС).

Применение комплексного метода построения ГЗОС позволит обеспечить 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». Сотрудник бизнес подразделения проводит идентификацию информационных активов, участвующих в бизнес процессах, которые планируется автоматизировать в рамках облачной среды. Сотрудник бизнес подразделения детализирует и подробно описывает бизнес процесс организации с обязательным указанием функций, отвечающих за обработку 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.

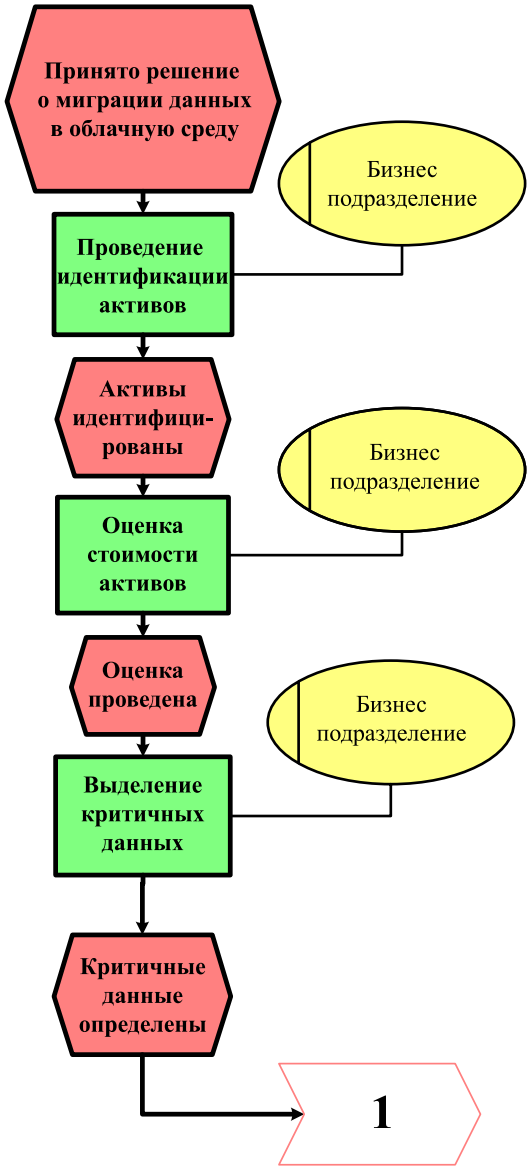

Рис. 1. Этап 1 «Идентификация и оценка критичных активов организации».

Этап 2 «Идентификация требований безопасности и определение последовательности обработки данных в ГЗОС». Сотрудник службы ИБ проводит идентификацию требований информационной безопасности ИТС, построенной на технологии облачных вычислений. Один из подходов к построению деревьев целей ИБ облачной инфраструктуры организации рассмотрен в работе [2]. Критериально-математический аппарат

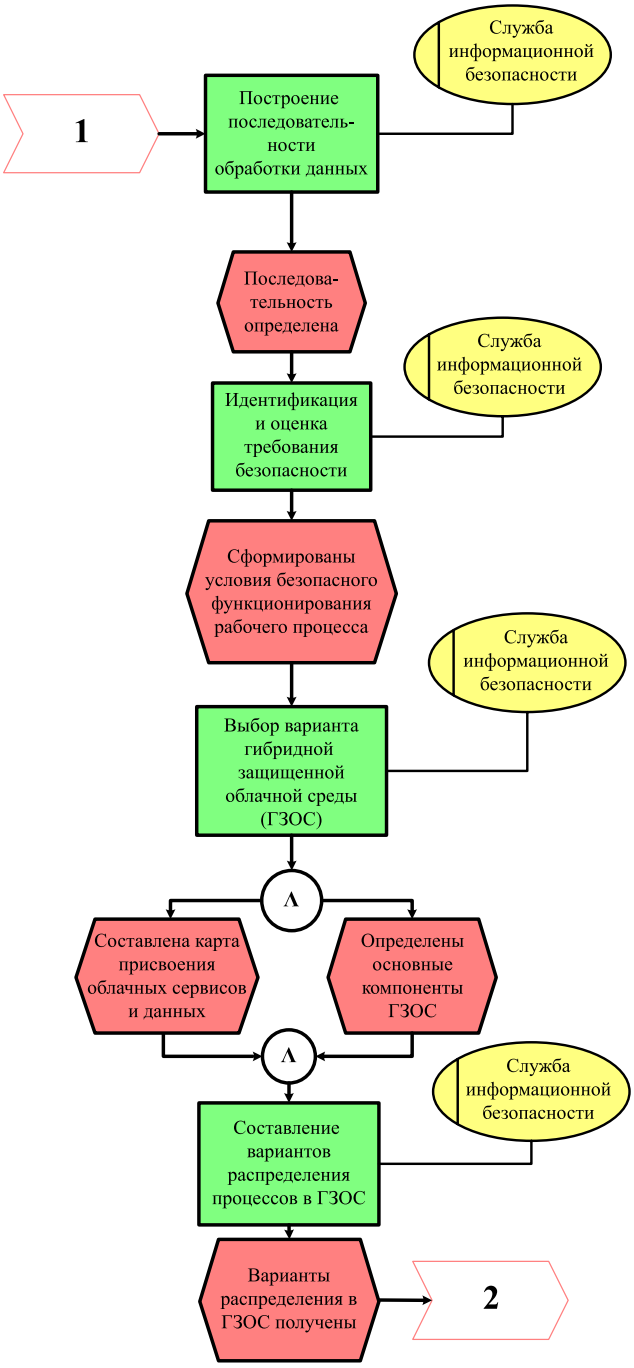

Рис. 2. Этап 2 «Идентификация требований безопасности и определение последовательности обработки данных в ГЗОС».

«измерения» свойства системности на деревьях целей на основе таких алгебраических объектов, как полугруппы с единицей — моноидов, подробно рассмотрен в [3].

Последовательность обработки критичных данных на базе формализованной модели безопасности процесса обработки данных в условиях среды облачных вычислений детально рассмотрена в работе [4].

Этап 3 «Идентификация угроз и построение риск модели ГЗОС». Управление информационными рисками является центральным процессом измерения различных показателей информационной безопасности. Для каждого информационного актива, нужно 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. Чтобы успешно реализовать все действия процесса анализа риска необходимо внедрить в организации процессы контроля и применения контрмер. Основные этапы процесса управления рисками и их реализация в современных инструментальных средствах показаны в работе [5].

Этап 4 «Применение стоимостной методики и построение архитектуры ГЗОС». Сотрудник службы ИБ на основании стоимостной методики получает стоимость различных вариантов развёртывания ГЗОС и на основании практических рекомендаций осуществляет выбор различных вариантов построения архитектуры ГЗОС.

Изменение контура безопасности, выход критичных активов организаций из-под внутреннего контроля с последующей миграцией этих активов в облачную среду поставил основную цель настоящего исследования, которая заключается в совершенствовании методов управления информационной безопасностью информационно-телекоммуникационных сред, функционирующих на основе технологии облачных вычислений. Достижение этой цели позволит существенно повысить эффективность использования ИТ-ресурсов и значительно сократить их стоимость за счет диверсификации информационных потоков организации при их миграции на гибридную защищенную облачную архитектуру.

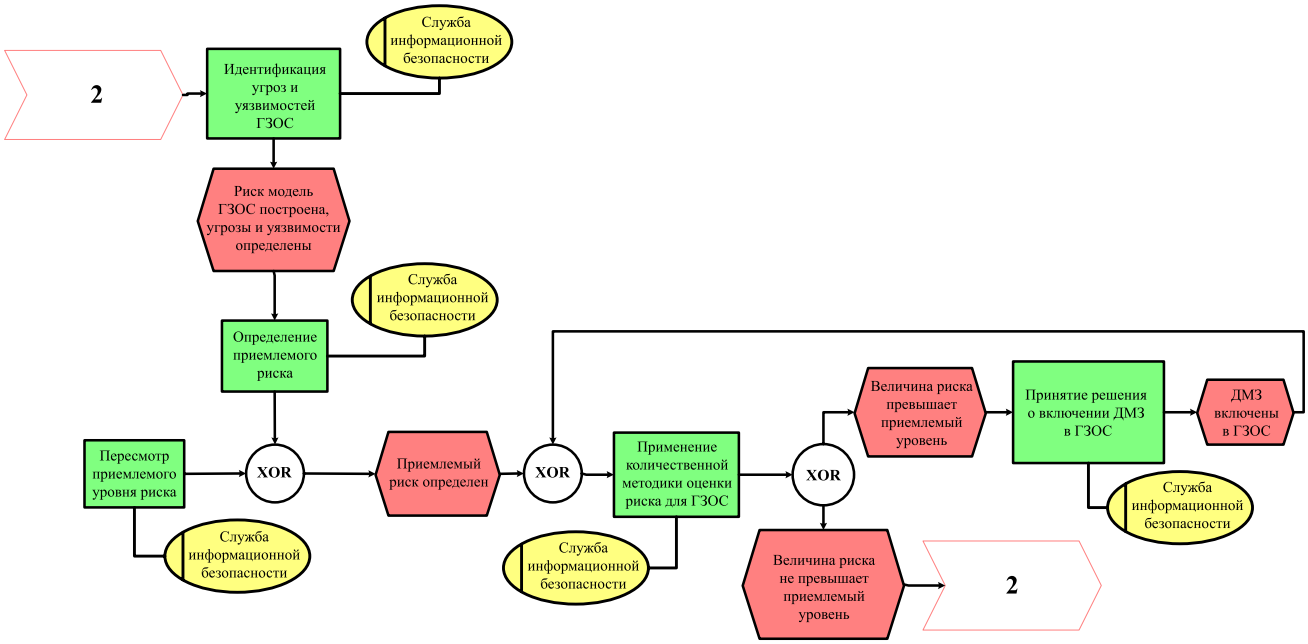

Рис. 3. Этап 3 «Идентификация угроз и построение риск модели ГЗОС».

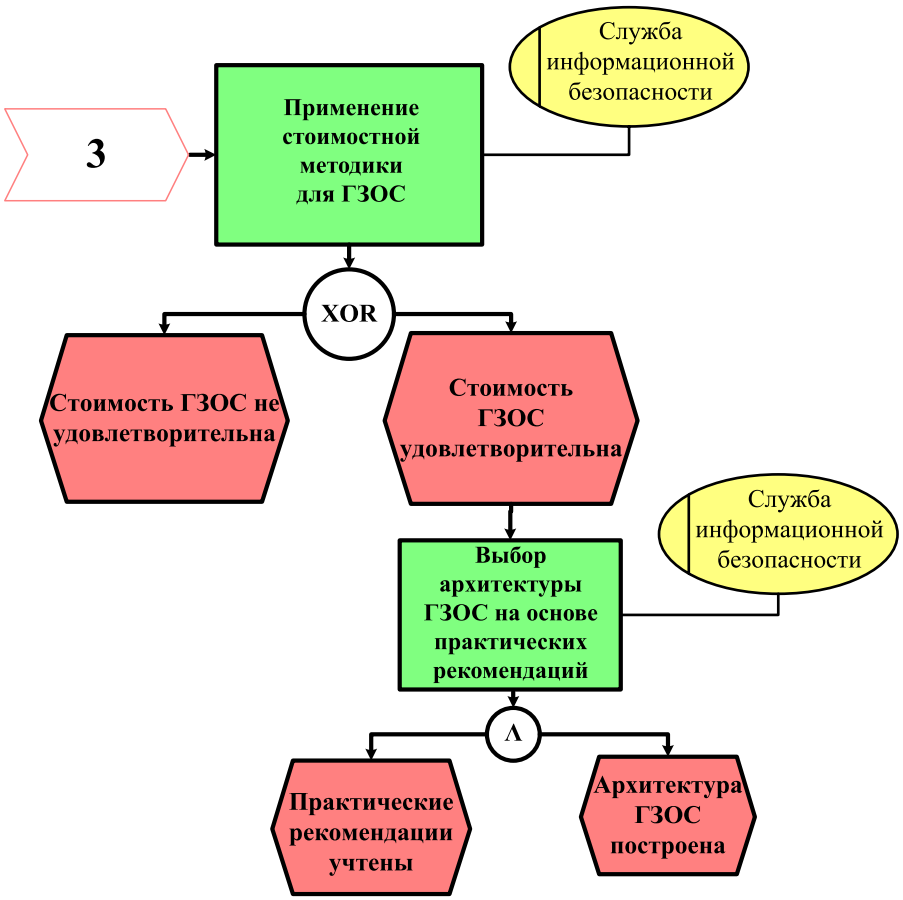

Рис. 4. Этап 4 «Применение стоимостной методики и построение архитектуры ГЗОС».

Список литературы

1. National Institute of Standards and Technology (NIST). Definition of Cloud Computing, http://csrc.nist.gov/groups/SNS/cloud-computing/
2. Качко А.К. Один из подходов к построению деревьев целей информационной безопасности для облачной инфраструктуры организации// Сборник материалов VIII Международной научно-практической конференции «Перспективы развития информационных технологий» – Новосибирск, С.25-30.
3. Царегородцев А.В. Монография «Теория построения иерархических информационно-управляющих систем». – 2004. - С. 217.
4. Качко А.К. Формализованная модель безопасности процесса обработки данных в условиях среды облачных вычислений//Проблемы информационной безопасности. Компьютерные системы. – 2012. – №2 –С. 14-20.
5. Малюк А.А., Горбатов В.С., Королев В.И., Фомичев В.М., Дураковский, А. П., Кондратьева Т. А. Введение в информационную безопасность // Горячая Линия - Телеком. - 2011. - С. 290.