А. К. Качко, М. М. Лавриненко, А. В. Царегородцев

ОДИН ИЗ ПОДХОДОВ К ПОСТРОЕНИЮ ГИБРИДНОЙ ЗАЩИЩЕННОЙ ОБЛАЧНОЙ СРЕДЫ

Введение

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 хорошему соотношению цена/качество [1].

При этом самыми критичными вопросами при построении инфраструктуры, основанной на среде облачных вычислений, являются аспекты обеспечения информационной безопасности. Достижение целей информационной безопасности организации — ключевой фактор для принятия решений об услугах аутсорсинга информационных технологий и, в частности, для принятия решения о миграции информационных активов организации на различные модели предоставления облачных сервисов. Большинство организаций не могут себе позволить защитить все свои вычислительные ресурсы и активы в силу бюджетных ограничений, поэтому при переходе на новую модель предоставления ИТ-услуг особое внимание должно уделяться вопросам обеспечения безопасности обработки информации [2].

1. Требования информационной безопасности облачных вычислений

Рассмотрим ряд факторов, которые должны всегда рассматриваться в качестве основы построения облачной архитектуры и отвечать требованиям соответствующих стандартов, например ISO 27001 и ISO 27002, так как они содержат практическую ценность, опыт, отчеты и рекомендации лучших практик.

Все аспекты безопасности должны быть отражены в документе **«Политика информационной безопасности организации»** («Политика облачной безопасности»), который имеет статус официального документа, согласовывается и утверждается высшим руководством. Политика безопасности должна рассматриваться как фундамент построения всей системы и не должна содержать подробных технических или архитектурных подходов (так как они могут меняться чаще, чем сама политика). Главная цель политики должна заключаться в определении основополагающих организационных и управленческих решений при построении комплексной безопасности облачной среды. Например, политика должна объяснить необходимость применения шифрования с помощью использования какого-либо коммерческого продукта, а не включать в себя техническое описание безопасности транспортного уровня, протоколы защиты информации или другие специальные средства.

Политика безопасности также должна иметь ссылки на следующие разделы [4]:

- Ряд руководящих принципов для обеспечения безопасности при разработке программного обеспечения, в процессах управления ИТ-инфраструктурой и других операционных процедурах.
- Политика допустимого использования ресурсов для каждой категории пользователя: от внутренних операций, выполняемых администратором, до действий конечных пользователей. Этот раздел должен идентифицировать категории использования ресурсов, определить критичную информацию, доступ к которой запрещен, обозначить последствия для нарушений.
- Ряд стандартов безопасности для всех аспектов облачной архитектуры — от миграции данных до операционной деятельности.

Стандарты безопасности для облачных вычислений должны включать в себя:

1) Средства управления доступом. Детализация целей данного уровня должна быть достаточной для осуществления контроля физического доступа к центрам обработки данных и логического доступа к системам и приложениям.

2) Управление реагированием на инциденты безопасности. Должно быть подробно описано назначение всех ролей и обязанностей различных сторон, наряду с процедурами и сроками обнаружения инцидентов.

3) Резервное копирование системной и сетевой конфигурации. Необходимо иметь гарантированно надежную копию всех конфигураций, включая компоненты инфраструктуры, серверы и другое сетевое оборудование для всех хост-систем.

4) Тестирование безопасности. Облачный провайдер должен выполнять и документировать результаты первоначального и периодического тестирования безопасности. Этот стандарт должен включать роли и обязанности, а также подробное описание, когда планируется проведение сторонних тестирований или аудита.

5) Шифрование данных и связи. Должны быть идентифицированы все функциональные области (например, веб-трафик сервера), утверждены криптографические алгоритмы и необходимая длина ключа шифрования.

6) Политика строгих паролей. Должны быть описаны ключевые аспекты при задании паролей (в частности, длина и состав) и как облачный провайдер будет проводить процедуру аутентификации.

7) Непрерывный мониторинг. Должно быть детально описано, как выполняется управление конфигурациями и изменениями (развитие и обновление) с целью поддержки требуемого уровня безопасности и сохранения ключевого требования к информационной безопасности — непрерывности бизнеса.

2. Метод построения системы защиты информации на облачной архитектуре

На сегодняшний день целый ряд открытых вопросов информационной безопасности не позволяет 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) характерны 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 серьезные 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 в облачную архитектуру необходимо, чтобы организация могла в полной мере обеспечить контроль над критичными активами, даже несмотря на большие финансовые издержки при эксплуатации ЧОС. 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 метод построения гибридной защищенной облачной среды (ГЗОС). Применение метода 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» — рис. 1. 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.

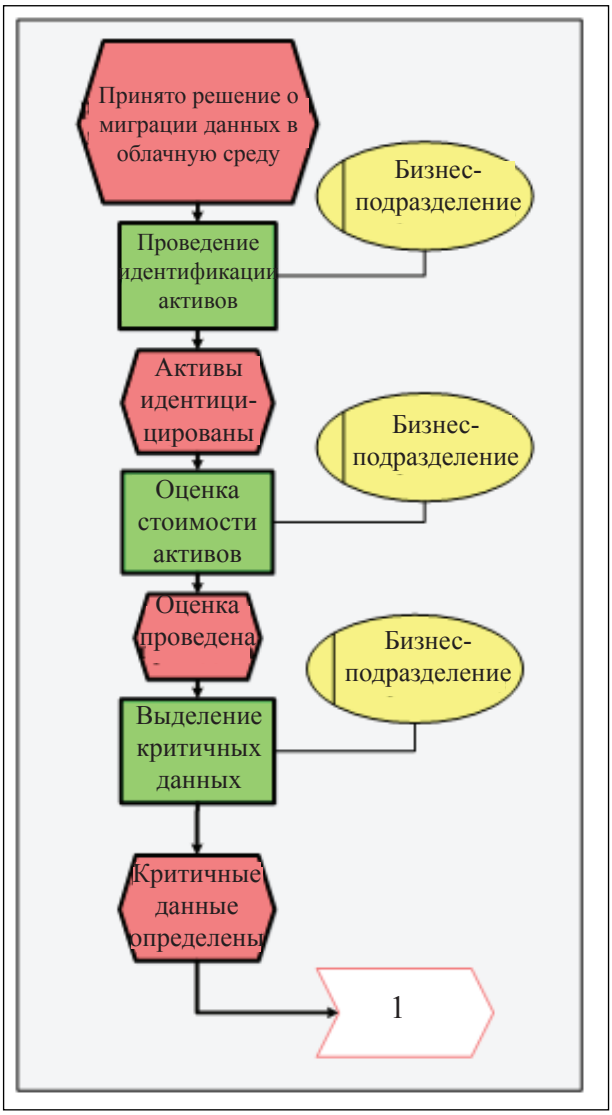

Рис. 1. Этап 1 «Идентификация и оценка критичных активов организации»

Этап 2 «Идентификация требований безопасности и определение последовательности обработки данных в ГЗОС» — рис. 2. Сотрудник службы ИБ проводит идентификацию требований информационной безопасности ИТ-системы, построенной на технологии облачных вычислений. Один из подходов к построению деревьев целей ИБ облачной инфраструктуры организации рассмотрен в работе [2]. Критериально-математический аппарат «измерения» свойства системности на деревьях целей на основе таких алгебраических объектов, как полугруппы с единицей — моноиды, 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].

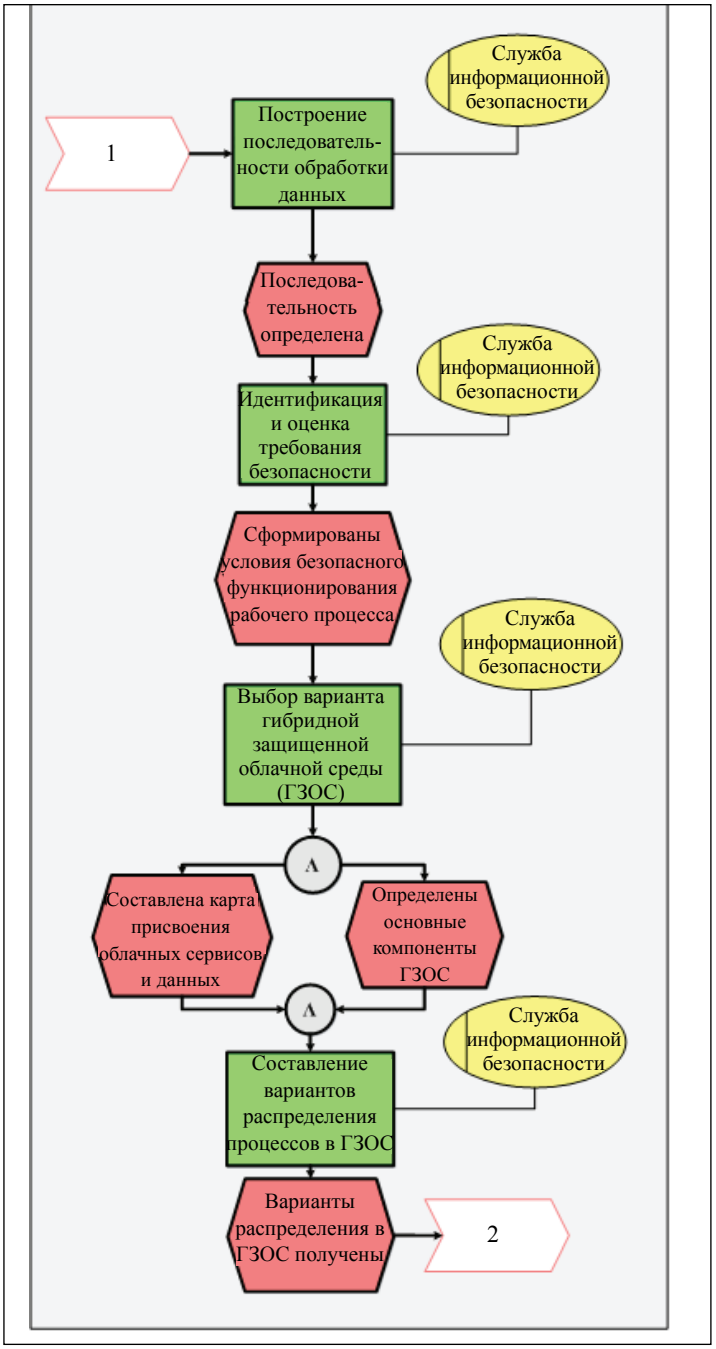

Рис. 2. Этап 2 «Идентификация требований безопасности и определение последовательности обработки данных в ГЗОС»

Этап 3 «Идентификация угроз и построение риск-модели ГЗОС» – рис. 3. 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.

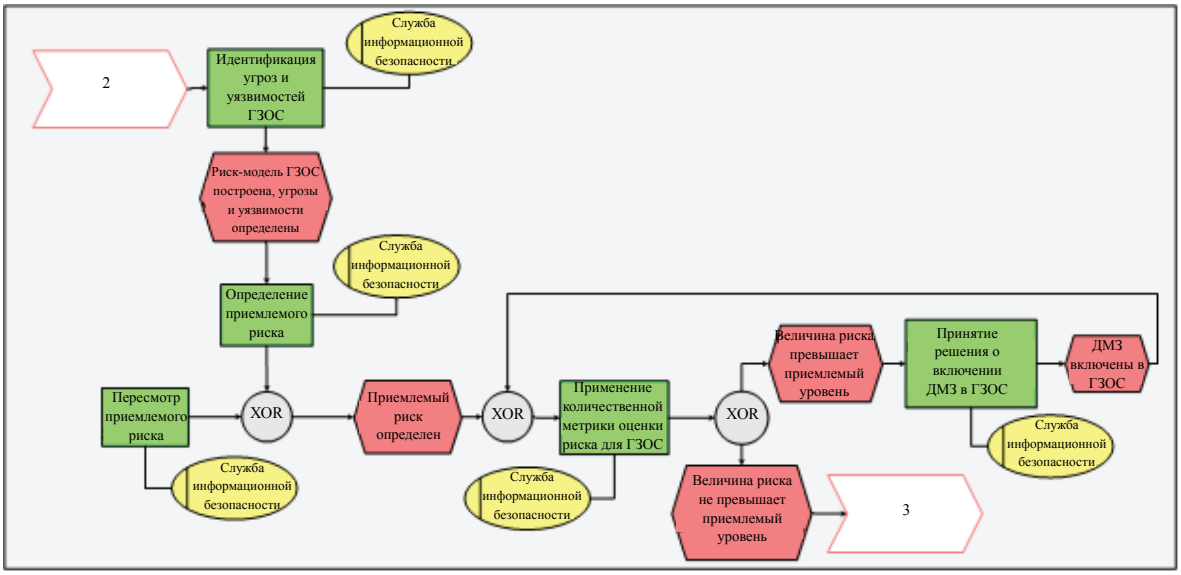

Рис. 3. Этап 3 «Идентификация угроз и построение риск-модели ГЗОС»

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

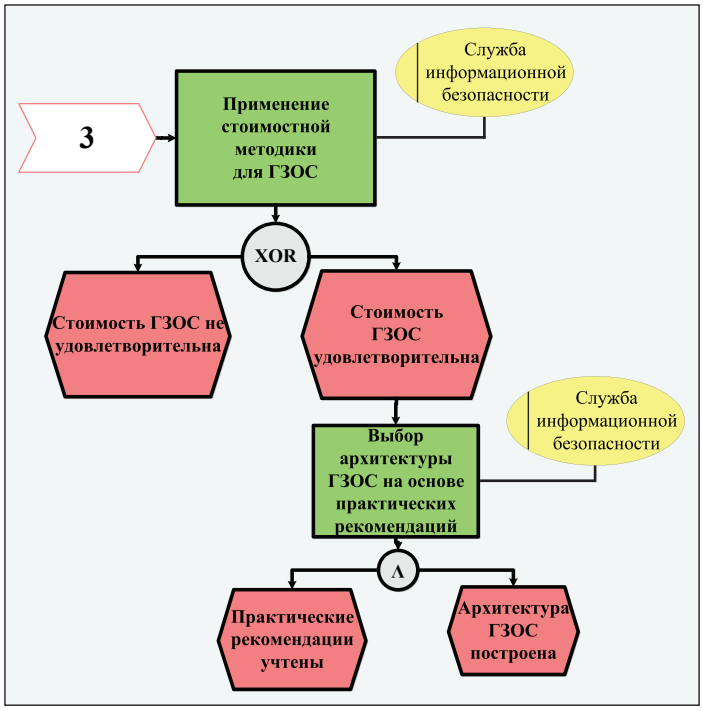

Рис. 4. Этап 4 «Применение стоимостной методики и построение архитектуры ГЗОС»

Заключение

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.

СПИСОК ЛИТЕРАТУРЫ:

1. National Institute of Standards and Technology (NIST). Definition of Cloud Computing. URL: http://csrc.nist.gov/groups/SNS/cloud-computing/ (дата обращения: 12.12.2013).
2. *Царегородцев А. В.* Построение деревьев целей для идентификации требований безопасности среды облачных вычислений // Национальная безопасность. 2013. № 5 (28). С. 51–69.
3. *Царегородцев А. В., Кислицын А. С.* Основы синтеза защищенных телекоммуникационных систем. М.: Радиотехника. 2006. – 244 с.
4. *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.