DOI: 10.7256/2073–8560.2013.5.9583

А.В. Царегородцев, Г.Н. Ермошкин

БАЗОВЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ ДЕРЕВА ЦЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Аннотация: *изменение контура безопасности и выход критичных активов организаций из-под внутреннего контроля с последующей миграцией этих активов в облачную среду выдвинули на первое место проблему управления информационной безопасностью корпоративных систем, функционирующих на основе технологии облачных вычислений. Все это требует пересмотра традиционных подходов к обеспечению информационной безопасности и разработки нового методологического аппарата, позволяющего существенно повысить эффективность использования IT ресурсов и значительно сократить их стоимость за счет диверсификации информационных потоков организации при их миграции на облачную архитектуру. Особое внимание в данной статье уделено открытым вопросам информационной безопасности и вариантам их решения на основе построения дерева целей информационной безопасности среды облачных вычислений. Предлагается новая концепция безопасности среды облачных вычислений на основе дерева целей, которая учитывает все критичные процессы управления информационной безопасности и позволяет принимать во внимание понятие «общей ответственности и общих обязанностей» сторон, что предоставляет возможность организациям принимать решение о развертывании информационной сети по критерию минимизации издержек на инфраструктуру с обеспечением необходимого уровня информационной безопасности.*

Ключевые слова: *информационная безопасность, облачные вычисления, облачные сервисы, угрозы информационной безопасности, дерево целей, методы управления, требования информационной безопасности, модель предоставления сервисов, контрмеры, бизнес процессы.*

Review: *changing security contour and loss of internal control over the critical assets of organizations followed by the later migration of these assets to the cloud spheres made the problem of information cloud computing security management in the corporate system a top priority issue. All of the above requires the change in the traditional approaches to the information security guarantees and development of the novel methodological apparatus, allowing for higher efficiency of the IT resources and considerably lowering their costs via diversification of information streams in the organization and their migration to the cloud architecture. Much attention is paid to the topical information security problems and their possible solutions based on formation of the trees of objectives for the information security in the cloud computing environment. The authors offer a novel concept for the cloud computing environment security based upon the tree of objectives, allowing to take into account all of the critical processes in the sphere of information security management, and to take into consideration the terms of common responsibility and common obligations of the parties, the above-mentioned qualities shall allow the organizations to make*

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2013.5.9583

decisions on the formation of information network based on the criterion of minimal infrastructure costs, while guaranteeing the necessary information security level.
Keywords: *information security, cloud computing, cloud services, information security threats, tree of objectives, management methods, information security requirements, service provision model, counter-measures, business processes.*

Введение

Сегодня достижение целей информационной безопасности организации является ключевым фактором при принятии решений об услугах аутсорсинга информационных технологий и, в частности, при принятии решения о миграции критически важных данных и приложений в информационно-телекоммуникационную систему, функционирующую на основе технологии облачных вычислений.

Многие из предоставляемых в настоящее время интерфейсов и сервисов среды облачных вычислений используют недекларированные механизмы защиты, поэтому при рассмотрении вопросов обеспечения комплексной информационной безопасности особое внимание уделяется:

- моделям предоставления облачных сервисов (SaaS, PaaS, IaaS);
- типам развёртывания облачной среды (общедоступное, частное, сообщество, гибридное).

Проведенный анализ показал, 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[1]. Что требует разработки новых методов формализованного синтеза платформ безопасности информационно-телекоммуникационных систем, функционирующих на основе технологии облачных вычислений, в соответствии с определяемыми критериями системности и с учётом фактора развития системы[2].

1. Отправные методологические положения для идентификации и оценки требований безопасности среды облачных вычислений

Необходимость совершенствования и повышения эффективности кардинальных принципов управления информационной безопасностью среды облачных вычислений приводит к многоаспектной области обеспечения свойств «системности»:

- упорядоченной целостности;
- самостабилизации;
- самоорганизации;
- иерархичности (при моделировании и синтезе).

Применение технологии и методов формализованного структурного синтеза систем управления информационной безопасностью (СУИБ) в облачной среде, соединяющих различную структуру иерархий требований, позволило бы с большей эффективностью воспользоваться уже разработанными в каждом из локальных обеспечений техноло-

[1] Отчёт ENISA: Облачные вычисления: Преимущества, риски и рекомендации по управлению безопасностью (2009) Технический отчёт, Европейское агентство по сетевой и информационной безопасности.

[2] Царегородцев А.В., Качко А.К. Обеспечение информационной безопасности на облачной архитектуре организации // Национальная безопасность.— М.: Изд-во «НБ Медиа», 2011.—№ 5.— С. 25–34.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2013.5.9583

гиями и средствами автоматизации свойств и проявлений системности[1].

Отличную возможность предоставляет эмпирически присущее моделям типа дерева целей свойство системности их структуры, которое имеет структурную адекватность взаимосвязи целого (вершины) и его частей (подцелей) в процессе декомпозиции или, наоборот, композиции требований информационной безопасности.

Возможность сведения ряда орграфов «древесного типа», имеющих петли или циклы (нелинейную структуру), к строгому дереву повышает актуальность разработки формальных методов синтеза систем управления безопасностью облачной среды на основе дерева целей. Это обстоятельство позволяет использовать дерево целей в качестве основной, системообразующей модели для СУИБ иерархического типа при разработке методов повышения структурной эффективности.

Опишем отправные методологические положения для идентификации и оценки требований безопасности среды облачных вычислений.

1. Структурная интеграция реализуется определением:

- дерева целей в качестве системообразующей модели,
- управляющих модулей, рассматриваемых в качестве целостных объектов формализованного проектирования — число, состав и содержание которых должно быть синтезировано непосредственно по дереву целей.

2. Этапы формализованной технологии системного синтеза управляющей структуры должны определяться на основе трёх уровней реализации концепции прямого синтеза:

- фазы задания свойства системности как исходного,
- фазы моделирования процесса его передачи по этапам и уровням проектирования,
- фазы определения собственно задач формализованной технологии синтеза и математических методов их решения.

3. Содержательная интерпретация модели первой фазы связана с выбором ориентации дуг дерева целей вверх. При этом понятию внешний функции системы можно сопоставить главную цель — вершину дерева, а понятию внутренней функции системы сопоставить процесс продуцирования целей своими подцелями.

4. Создание формальной модели должно исходить из концепции продуцирования целей своим подцелям.

Критериально-математический аппарат «измерения» свойства системности на деревьях целей на основе таких алгебраических объектов, как полугруппы с единицей — моноидов, подробно рассмотрен в работе [4][2].

Определим ключевые организационно-правовые вопросы для построения эффективной системы управления информационной безопасности и рассмотрим ряд контролей, которые должна учитывать организация, прежде чем принимать решение о миграции данных в среду облачных вычислений.

1. Согласование контрактных соглашений между провайдером и клиентом.

1.1. Определение ответственных лиц за владение активами организации в облачной среде.

[1] Оунс С. (2010) Эластичная безопасность в облачных технологиях. Издательство Commun ACM 53 (6): С. 46–51.

[2] Царегородцев А.В., Кислицын А.С. Основы синтеза защищенных телекоммуникационных систем.— М.: Радиотехника, 2006.—244 с.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2013.5.9583

1.2. Согласование процедур, позволяющих осуществление перехода к другому провайдеру.
1.3. Определение прав и возможностей сторон для оперативного принятия контрмер в случае нарушения информационной безопасности и появлении инцидентов.
2. Проведение сертификации и аудита третьей стороной по запросу клиента.
2.1. Планирование и выбор сертификации для облачного провайдера.
2.2. Возможность проведения независимого аудита объектов инфраструктуры со стороны клиента.
3. Соответствие требованиям нормативно-правовых и законодательных актов РФ.
3.1. Определение физического места расположения инфраструктуры провайдера.
3.2. Соблюдение и принятие во внимание права правоохранительных органов потребовать полный доступ к информации организации с последующим раскрытием информации со стороны провайдера без согласия клиента.
4. Обеспечение доступности, целостности и конфиденциальности данных со стороны провайдера.
a. Обеспечение доступности, целостности и конфиденциальности критических данных во время недоступности облачного сервиса.
b. Наличие возможностей для получения доступа при отказе оборудования провайдера предоставить штатные точки доступа к информационным ресурсам организации.
5. Осуществление резервного копирования и восстановления данных в случае физического или логического сбоя.
5.1. Определение временного периода для восстановления данных и возобновления штатной работы со стороны провайдера.

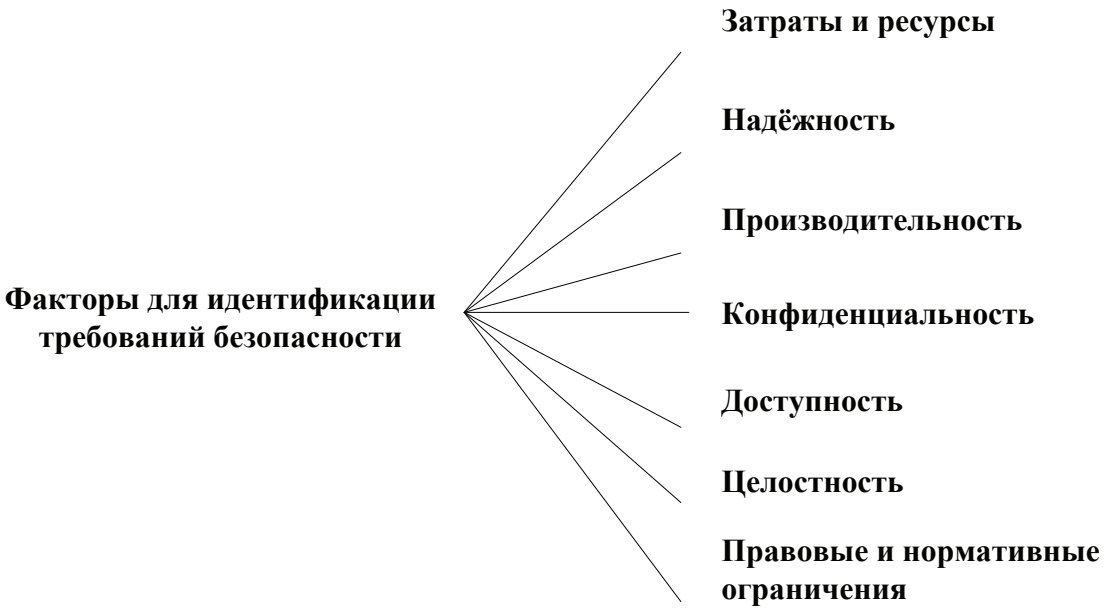

Рис. 1. Факторы для формирования требований информационной безопасности облачной среды

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2013.5.9583

5.2. Определение контролей для проверки работоспособности восстановленной копии со стороны клиента.
6. Согласование процедур облуживания и поддержка производительности.
6.1. Согласование вариантов решения вопросов по увеличению производительности облачных сервисов на пике загрузки вычислительных мощностей провайдера.
7. Определение процедур удаление критичной информации и вывод из эксплуатации избыточных ресурсов.
8. Оптимальное использование виртуальных машин и процессов.

Проведенный анализ существующих моделей предоставления облачных сервисов позволяет определить классификацию требований информационной безопасности в виде дерева целей, которое должно основываться на принципах достаточности определенного уровня защиты для активов организации. На рисунке 1 показаны высокоуровневые факторы, позволяющие определить необходимый набор требований информационной безопасности среды облачных вычислений.

Детализируем факторы и докажем необходимость их учёта при идентификации требований среды облачных вычислений.

Затраты и ресурсы. С одной стороны финансовые возможности облачного провайдера ограничивают его в возможностях совершенствовать процедуры и механизмы обеспечения информационной безопасности. Отсутствие неограниченных ресурсов может мотивировать провайдера серьёзно подойти к вопросам проектирования, построения архитектуры и выбора оптимального решения для клиента. С другой стороны уменьшение стоимости ИТ решения — это главная мотивация для потребителя облачных услуг. Природа этих ограничений приводит к развитию сервисов с характеристиками, которые нельзя применить для покрытия требований разных клиентов, что ведёт к необходимости создавать уникальные и эффективные проектные решения в каждом конкретном случае.

Надёжность. Свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования.

Производительность. Совокупность нескольких свойств, которые имеют отношение к полезности системы. К примеру, общие меры включают оперативность реагирования на входную информацию (чувствительность) и пропускную способность системы при обработке.

Целостность. Конфиденциальность. Доступность. Это основные принципы информационной безопасности для всех типов систем, главная цель при построении комплексной защиты — это соотнесение их с показателями надежности, производительности и стоимости решения.

Правовые и нормативные ограничения. Нормативно-правовые ограничения могут привести к необходимости учета дополнительных требований, связанных с техническими контролями безопасности, политики доступа, хранения данных.

2. Базовые принципы построения дерева целей информационной безопасности среды облачных вычислений

С использованием общедоступных облачных сервисов большая часть сети, систем, приложений и данных организации будет перенесена на контроль сторонней организации — облачного провайдера. Различные

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2013.5.9583

модели предоставления облачных сервисов выстраивают виртуальное пространство для клиента, в котором необходимо чётко разделить обязанности между клиентом и провайдером. Эта модель общей ответственности создает новое направление для формирования требований безопасности всей облачной среды.

Первый вопрос, на который необходимо дать ответ, это соответствует ли уровень прозрачности облачных сервисов уровню управления (распределению ответственности), а так же соответствует ли требованиям безопасности процессы для предоставления гарантий бизнесу, что информация на облаках соответствующе защищена[1].

Для ответа на данный вопрос, необходимо определить какие требования безопасности должен учитывать провайдер со своей стороны, и как должны быть применены традиционные элементы и процессы управления безопасностью организации в новой

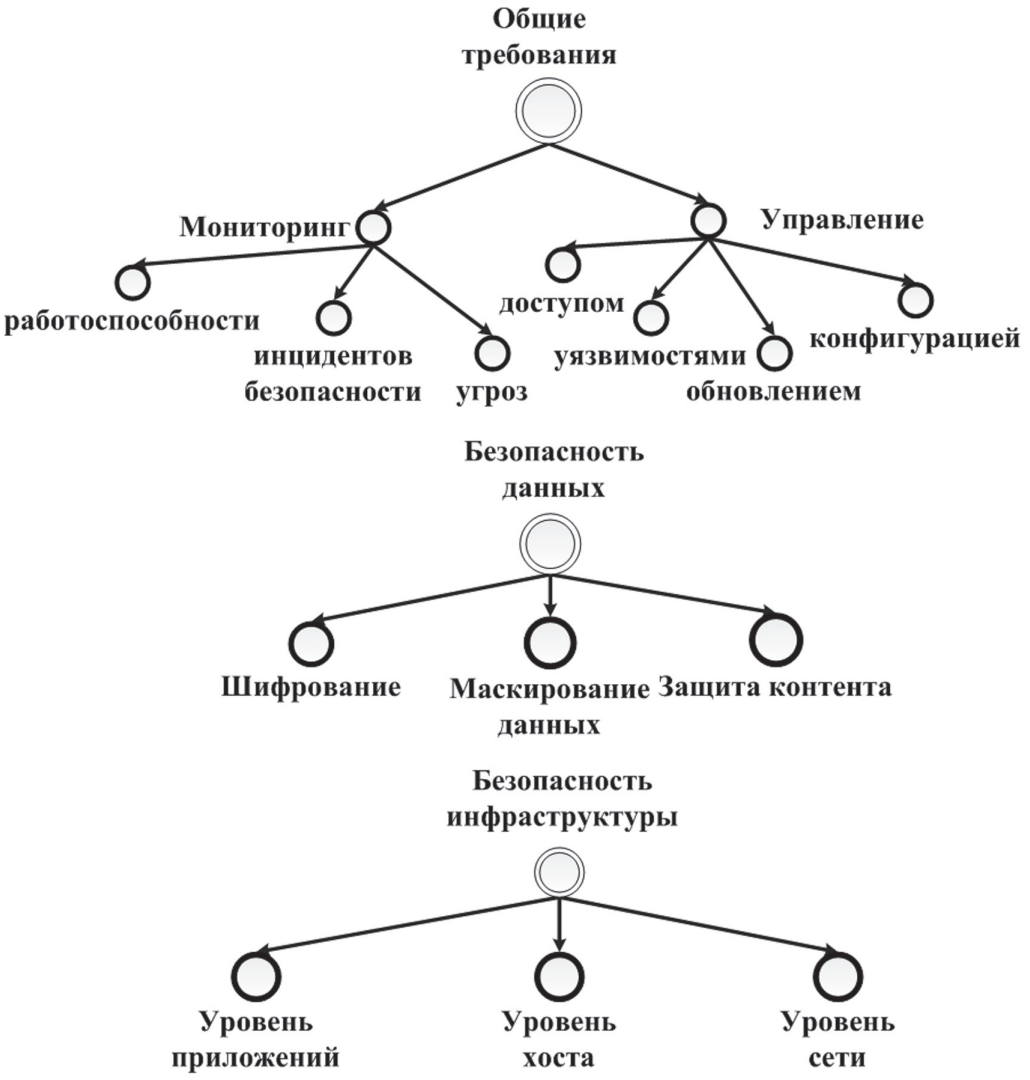

Рис. 2. Дерево целей требований безопасности облачной среды

[1] Чен И. Пэксон И., Пэксон В., (2010) Новые проблемы информационной безопасности облаков. Технический отчёт UCB/EECS-2010–5, Департамент EECS, Университет Калифорнии, Беркли.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2013.5.9583

облачной среде. Оба ответа должны быть основаны на постоянной оценке критичности и значимости данных и сервисов, а так же на изменении уровня обслуживания с течением времени.

Клиент должен понимать границы доверия для обработки своих данных на всех уровнях облачной архитектуры: сеть, хост, приложение, база данных, хранилище данных и веб-сервисы, включая услуги проверки подлинности (см. рисунок 2). Важным элементом для выстраивания инфраструктуры с разделением полномочий и общей ответственностью становится понимание требований безопасности для управления доступом, изменениями и конфигурацией, управлением обновлением, патчами и уязвимостями.

С одной стороны возможно перенесение ответственностей за обеспечение безопасности всех операций на сторону провайдера, тогда уровень ответственности будет зависеть от:

- модели предоставляемых услуг;
- соглашения об уровне обслуживания;
- возможностей провайдера поддерживать внутренние процессы и инструменты управления безопасностью организации.

Крупные организации применяют лучшие практики управления безопасностью, такие как: ISO/IEC 27000 и Библиотеку инфраструктуры информационных технологий (ITIL). Эти производственные стандарты систем управления предоставляют руководство к планированию и осуществлению управленческих программ с поддержкой управления процессами, которые защищают информационные активы. Например, ITIL предоставляет детализированное описание некоторых важных норм с всеобъемлющим перечнем заданий и процедур, которые могут быть применены для любой организации в сфере IT. Ключевой принцип ITIL, который применим к облачным вычислениям, заключается в том, что организации (люди и процессы) и информационные системы должны постоянно изменяться. В связи с этим инфраструктуры управления, такие как ITIL, помогают непрерывно повышать качество предоставляемых услуг, которые необходимы для установки и реконструкции IT услуг для изменения бизнес потребностей. Непрерывное повышение качества предоставляемых услуг означает определение и внедрение IT услуг, поддерживающих бизнес процессы. Учитывая динамические характеристики услуг облачных вычислений, подобная деятельность, присутствующая в процессах управления безопасностью, должна постоянно пересматриваться, чтобы сохранять свою своевременность и эффективность.

Управление безопасностью — это постоянный процесс, являющийся очень важной частью системы управления безопасностью в облачных вычислениях. Задача инфраструктуры управления безопасностью ITIL разделена на две части.

1. Реализация требований безопасности.
2. Требования безопасности обычно определяются в SLA, а так же в порядке внешних требований, которые указаны в основах договоров, законодательств, внутренней и внешней политики.

Реализация базового уровня безопасности.

Необходимо для гарантий безопасности, обеспечения непрерывности бизнеса организации, достижения упрощенного уровня управления информационной безопасностью облачной среды.

Устоявшееся управление безопасностью процессов так же приведено в соответствие с политикой и стандартами IT организации, с целью защиты конфиденциальности, целостности и доступности информации.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2013.5.9583

Дисциплины управления безопасностью представлены соответствующим ISO и ITIL функциям.

Таким образом, стандарты ITIL и ISO/IEC 27001 и 27002 имеют прямое отношение к практике управления безопасности среды облачных вычислений. Для целей нашего исследования рассмотрим основные положения приведенных стандартов.

ITIL. Библиотека инфраструктуры информационных технологий (ITIL) представляет собой набор лучших практик и руководств, которые определяют интегрированный подход на основе процессов управления услугами информационных технологий. Информационная безопасность рассматривается как повторяющийся процесс, который необходимо контролировать, планировать, реализовывать, оценивать и поддерживать.

Процесс управления безопасностью ITIL основывается на стандарте управления информационной безопасностью, так же известный, как ISO/IEC 17799:2005. Процесс управления безопасностью ITIL заключается в управлении уровнем обслуживания сервиса, в процессе управления инцидентами и процессе управления изменениями, так как они оказывают большое влияние на состояние безопасности системы (сервер, сеть или приложения). ITIL связан с первым международным стандартом управления безопасностью ISO/IEC 20000. Организации и системы управления не могут получить сертификат «ITIL-совместимый», но они могут добиться соблюдения и получения сертификации по ISO/IEC 20000, если они в своей основе используют ITIL как руководство в ITSM.

ISO 27001/27002. ISO/IEC 27001 формально определяет обязательные требования для систем управления информационной безопасностью (ISMS). Это так же и основа для стандартов сертификации, которые используют ISO/IEC 27002 для указания подходящих контролей информационной безопасности в пределах ISMS. Однако, поскольку ISO/IEC 27002 — это просто свод практик и руководств, а не стандарт сертификации, организации вольны выбирать и осуществлять контроль по своему усмотрению. По существу, рамки ITIL, ISO/IEC 20000 и ISO/IEC 27001/27002 помогают IT организациям усваивать и ответить на основные вопросы, такие как:

- обеспечивается ли необходимый уровень информационной безопасности,
- обеспечивается ли базовая защита всех операций и сервисов.

Основываясь на результатах анализа управленческих процессов по ITIL и ISO, предлагается определить следующие рекомендуемые процессы обеспечения безопасности сервисов в среде облачных вычислений (в скобках указан источник требований).

1. Управление доступностью (ITIL);
2. Контроль доступа (ISO/IEC 27002, ITIL);
3. Контроль уязвимостей (ISO/IEC 27002);
4. Управление обновлениями (ITIL);
5. Управление конфигураций (ITIL);
6. Реагирование на инциденты (ISO/IEC 27002);
7. Использование систем и мониторинга доступа (ISO/IEC 27002).

Выбор основывался на соображениях обеспечения необходимого уровня безопасности облачных сервисов по критерию минимума общего риска для организации. Другие области управления ITIL, такие как: обеспечение непрерывности бизнеса, будут иметь косвенное отношение к формированию технических требований. В табл. 1 показаны функции управления безопасностью, доступные в рамках разных моделей предоставления сервисов и типов развёртывания.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2013.5.9583

ТАБЛИЦА 1. ФУНКЦИИ БЕЗОПАСНОСТИ ДЛЯ РАЗНЫХ МОДЕЛЕЙ И ТИПОВ РАЗВЁРТЫВАНИЯ СРЕДЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Модель предоставления сервисов	Общедоступные облака	Частные облака
Программное обеспечение как услуга (SaaS)	1. Управление доступом (частично); 2. Мониторинг использования систем и доступа (частично); 3. Реагирование на инциденты.	Следующие функции управляются отделом управления безопасностью организации: 1. Управление доступностью. 2. Контроль доступа. 3. Управление уязвимостями. 4. Управление обновлениями. 5. Управление конфигураций. 6. Реагирование на инциденты. 7. Мониторинг использования системы и доступа.
Платформа как услуга (PaaS)	Следующие функции ограничены для пользовательских приложений развернутых на PaaS. Провайдер отвечает за платформу PaaS: 1. Управление доступностью. 2. Контроль доступа. 3. Контроль уязвимостей. 4. Управление обновлениями. 5. Управление конфигурацией. 6. Реагирование на инциденты. 7. Мониторинг использования системы и доступа.	
Инфраструктура как услуга (IaaS)	1. Управление доступностью (виртуально); 2. Контроль доступа (пользователями и ограниченной сетью); 3. Контроль уязвимостями (операционная система и приложения); 4. Управление обновлениями (операционная система и приложения); 5. Управление конфигурациями (операционная система и приложения); 6. Реагирование на инциденты; 7. Мониторинг использования систем и доступа (операционные системы и приложения).	

Принимая во внимание детальный анализ построенного дерева целей (рисунок 3), можно предположить, что организации сталкиваются с необходимостью расширять возможности прямого управления функциями безопасности общедоступного облака под определенные задачи и использовать процессы внутреннего управления, развивая частные облачные сервисы, тем самым создавая особый гибридный вид развёртывания среды облачных вычислений.

Заключение

В статье были рассмотрены общие и специфические вопросы обеспечения информационной безопасности облачных вычислений, и выделены области, которые непосредственно управляются со стороны облачного провайдера.

Проведенный анализ существующих моделей предоставления облачных сервисов позволил определить классификацию

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2013.5.9583

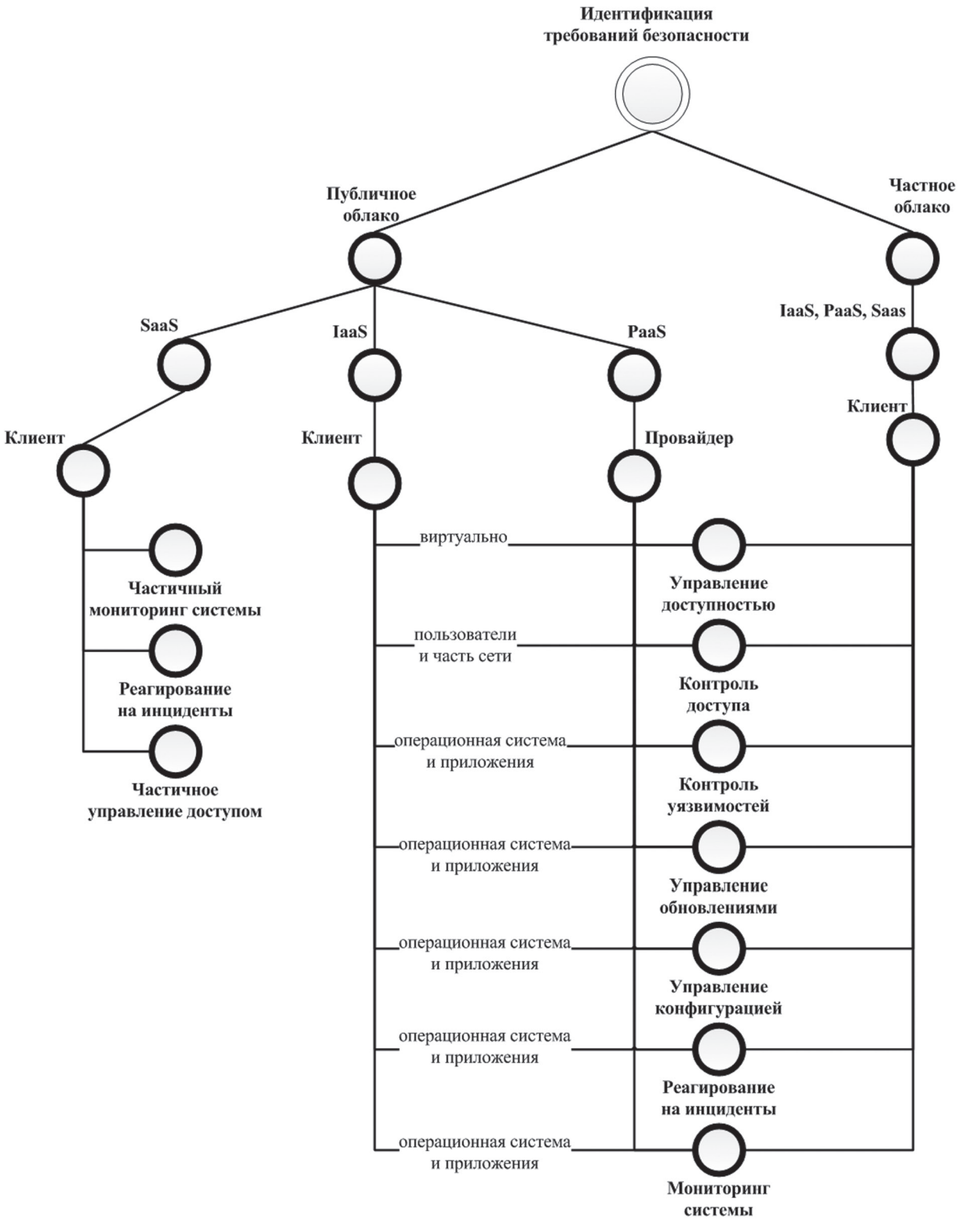

Рис. 3. Дерево целей требований безопасности облачной среды в разрезе типов облаков и моделей предоставления сервисов

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2013.5.9583

требований информационной безопасности в виде дерева целей, которое основывается на принципах достаточности определенного уровня защиты для активов организации. Различные модели предоставления облачных сервисов выстраивают виртуальное пространство для клиента, в котором необходимо чётко разделить обязанности между клиентом и провайдером. Эта модель общей ответственности создает новое направление для формирования требований безопасности всей облачной среды.

Важным элементом для выстраивания инфраструктуры с разделением полномочий и общей ответственностью становится понимание требований безопасности для управления доступом, изменениями и конфигурацией, управлением обновлением, патчами и уязвимостями.

Предложена новая концепция безопасности среды облачных вычислений на основе дерева целей, которая учитывает все критичные процессы управления информационной безопасности по критерию минимума общего риска для организации.

Библиография

1. Отчёт ENISA: Облачные вычисления: Преимущества, риски и рекомендации по управлению безопасностью (2009) Технический отчёт, Европейское агентство по сетевой и информационной безопасности.
2. Царегородцев А. В., Качко А. К. Обеспечение информационной безопасности на облачной архитектуре организации // Национальная безопасность.— М.: Изд-во «НБ Медиа», 2011.—№ 5.— С. 25–34.
3. Оунс С. (2010) Эластичная безопасность в облачных технологиях. Издательство Commun ACM 53 (6): С. 46–51.
4. Царегородцев А. В., Кислицын А. С. Основы синтеза защищенных телекоммуникационных систем.— М.: Радиотехника, 2006.—244 с.
5. Чен И. Пэксон И., Пэксон В., (2010) Новые проблемы информационной безопасности облаков. Технический отчёт UCB/EECS-2010–5, Департамент EECS, Университет Калифорнии, Беркли.

References (transliterated)

1. Otchet ENISA: Oblachnye vychisleniya: Preimushchestva, riski i rekomendatsii po upravleniyu bezopasnost'yu (2009) Tekhnicheskii otchet, Evropeiskoe agentstvo po setevoi i informatsionnoi bezopasnosti.
2. Tsaregorodtsev A. V., Kachko A. K. Obespechenie informatsionnoi bezopasnosti na oblachnoi arkhitekture organizatsii // Natsional'naya bezopasnost'.— M.: Izd-vo «NB Media», 2011.—№ 5.— S. 25–34.
3. Ouns S. (2010) Elastichnaya bezopasnost' v oblachnykh tekhnologiyakh. Izdatel'stvo Commun ACM 53 (6): S. 46–51.
4. Tsaregorodtsev A. V., Kislitsyn A. S. Osnovy sinteza zashchishchennykh telekommunikatsionnykh sistem.— M.: Radiotekhnika, 2006.—244 s.
5. Chen I. Pekson I., Pekson V., (2010) Novye problemy informatsionnoi bezopasnosti oblakov. Tekhnicheskii otchet UCB/EECS-2010–5, Departament EECS, Universitet Kalifornii, Berkli.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com