УДК 004.056
DOI: 10.24160/1993-6982-2018-3-126-131

Разработка модели безопасной информационной системы, использующей облачные сервисы

М.Т. Нгуен, П.Б. Хорев

Цель проведенной работы — предоставление разработчикам корпоративных информационных систем, использующих облачную инфраструктуру, возможности сократить время на обеспечение информационной безопасности при построении подобной системы. Проанализированы основные виды облаков, возникающие при их использовании риски информационной безопасности и модели предоставления услуг облачных сервисов. Облако рассмотрено с архитектурной точки зрения. Предложена обобщенная модель безопасной информационной системы с учетом существующих на данный момент информационных рисков. Сформулирована идея внедрения в модель шаблонов, содержащих классификацию и характеристики информационных рисков. Представлен неориентированный граф со структурой облака.
В результате использования разработанной модели появляется возможность получения качественной оценки информационных рисков, характерных для корпоративных информационных систем с облачными сервисами.

Ключевые слова: информационные технологии, безопасность и риски, облачные вычисления, угрозы в облачной среде.

Для цитирования: Нгуен М.Т., Хорев П.Б. Разработка модели безопасной информационной системы, использующей облачные сервисы // Вестник МЭИ. 2018. № 3. С. 126—131. DOI: 10.24160/1993-6982-2018-3-126-131.

Developing the Model of a Secure Information System That Uses Cloud Services

M.T. Nguyen, P.B. Khorev

The aim of the study is to offer to the developers of corporate information systems that use the cloud infrastructure the possibility to reduce the time taken to ensure information security in constructing such a system. The main types of clouds, the risks to information security arising from their use, and the models of providing cloud services are analyzed. A cloud is considered from an architectural point of view. A generalized model of a secure information system using cloud services is proposed that takes into account the currently existing information risks. The idea of incorporating patterns containing the classification and characteristics of risks into the model is formulated. An undirected graph with the cloud structure is presented.
The use of the developed model opens the possibility to obtain a qualitative assessment of information risks typical for corporate information systems with cloud services.

Key words: information technologies, security and risks, cloud computations, threats in the cloud environment.

For citation: Nguyen M.T., Khorev P.B. Developing the Model of a Secure Information System That Uses Cloud Services. MPEI Vestnik. 2018;3:126—131. (in Russian). DOI: 10.24160/1993-6982-2018-3-126-131.

Введение

За последние несколько лет облачные вычисления стали наиболее популярными и востребованными в различных информационных системах. Наиболее важными преимуществами облачных сервисов являются доступность информационных ресурсов, упрощение разработки информационных систем, мобильность, экономичность и др.

Облачные сервисы могут включать в себя еще и несколько суб-уровневых видов услуг. В соответствие с прогнозами на 2017 и последующие годы можно ожидать кардинальных перемен в том, как облачные вычисления будут использоваться в корпоративных информационных системах [1].

Несмотря на постоянное развитие облачных технологий, проблема информационной безопасности (ИБ) при работе с облачными сервисами остается актуальной. Существующие модели облачных вычислений редко рассматривают проблему безопасности как важную часть построения ИТ-инфраструктуры и не всегда учитывают специфику существующих угроз.

Необходима разработка модели безопасной информационной системы, использующей облачные сервисы. Цель ее создания состоит в том, чтобы предоставить разработчикам корпоративных информационных систем (КИС), использующих облачную инфраструктуру, возможность сократить время на обеспечение информационной безопасности. В результате использования разработанной модели появится возможность

получения качественной оценки информационных рисков, характерных для КИС с облачными сервисами.

Классификация облаков и моделей обслуживания

Облака делятся на 4 типа по характеру их владения (рис. 1), в каждом из которых есть свои конкретные преимущества и недостатки:

- частное (Private Cloud);
- общественное (Community Cloud);
- публичное (Public Cloud);
- гибридное (Hybrid Cloud).

Из основных моделей обслуживания выделяют три (вместе их еще называют SPI-моделями облачных сервисов):

- программное обеспечение (ПО) как услуга (SaaS);
- платформа как услуга (PaaS);
- инфраструктура как услуга (IaaS).

Модель SaaS освобождает заказчика от затрат, поскольку не требует установки, обновления и поддержки работоспособности оборудования и работающего на нем ПО. Другими словами, все основные затраты возлагаются на поставщика, а заказчику всего лишь надо иметь соответствующее клиентское устройство с доступом к функционалу облака. В связи с этим защита от возможных угроз ИБ является полностью задачей поставщика.

Модель PaaS, в отличие от модели SaaS, возлагает на поставщика ответственность только за физическую инфраструктуру вместе с администрированием на уровне операционных систем (ОС). На долю заказчика падает управление приложениями, развернутыми на базе данной инфраструктуры.

Модель IaaS позволяет заказчику арендовать вычислительные ресурсы, используемые им для установки и настройки любого ПО. Остальные же задачи в плане администрирования серверного и сетевого оборудования решает провайдер.

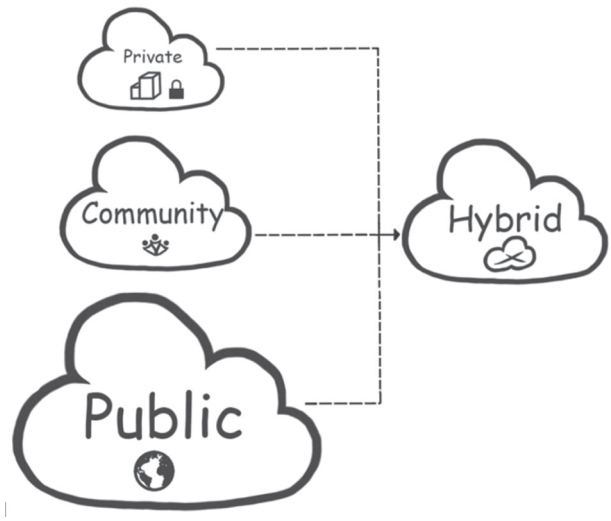

Рис. 1. Модели развертывания облака

Разница в распределении управления между заказчиком и поставщиком предоставляемых услуг содержится в табл. 1.

В той или иной модели часто появляются новые суб-модели услуг, но при рассмотрении ИБ достаточно и основных трех, так как по большей части их объединяют схожие информационные риски.

Таблица 1

Разница моделей SPI

Модели	SaaS	PaaS	IaaS
Приложения	P	C	C
Данные	P	C	C
Среда выполнения	P	P	C
Middleware	P	P	C
ОС	P	P	C\P
Виртуализация	P	P	P
Сервера	P	P	P
Хранилища	P	P	P
Сеть	P	P	P

Примечание. P — поставщик; C — клиент

Риски при использовании облачных сервисов

Выделим категории и подкатегории рисков, преобладающие в каждой из моделей SPI (табл. 2) [2 — 6].

Из табл. 2 следует, что модели PaaS и IaaS имеют риски технического характера, а модель SaaS — субъективного. Как уже было сказано, в модели SaaS ответственность полностью возлагается на поставщика, что объясняет существование рисков, связанных с прямым воздействием на инфраструктуру, потерей контроля и действиями возможных инсайдеров/злоумышленников, тем не менее, в зависимости от вида используемых облаков, такие же проблемы могут встречаться и при работе с другими моделями обслуживания, не говоря уже о вопросах правового обеспечения информационной безопасности [6].

Модель безопасной информационной системы на основе облака

Создание модели безопасной облачной системы требуется начать с анализа структуры облака, так как проявление многих информационных рисков тесно связано с уровнем поддержки оборудования, надежности каналов передачи данных, а также уровнем управления поставщиков и осведомленностью заказчиков, использующих облачные услуги.

Были использованы актуальные материалы по облачным вычислениям, включающие в себя такие вопросы как информационные риски, математические модели облачных центров обработки данных (ЦОД), транзакционные ИС и др. В связи с ограничением

Таблица 2

Категории рисков, присущие моделям SPI

SaaS	**Эксплуатационные проблемы:** ● изоляция данных, потеря ключа шифрования; ● банкротство поставщика **Неправильное управление данными:** ● риски локальности данных (место хранения); ● контроль идентификации; ● контроль целостности; ● контроль учета событий; ● регистрация действий клиентов; ● превышение полномочий поставщика; ● отсутствие поддержки поставщика
PaaS	**Общие проблемы безопасности:** ● проблемы, связанные с сервис-ориентированной архитектурой (SOA); ● проблемы, связанные с программным интерфейсом (API) **Эксплуатационные проблемы:** ● отсутствие взаимодействия между облачными провайдерами и унаследованными системами
IaaS	**Общие проблемы безопасности:** ● безопасность виртуальных машин (ВМ); ● безопасность гипервизора; ● безопасность хранилищ образов ВМ **Эксплуатационные проблемы:** ● ограничения ВМ; ● идентификация источников данных; ● инструменты обеспечения безопасности у поставщиков
Общие	**Общие проблемы безопасности:** ● общая безопасность данных; ● проблемы, возникающие при развитии и эволюции технологии облаков; ● естественные (устаревшее оборудование, природные факторы и т;д;) **Возможные атаки на облачный сервис извне/изнутри:** ● несанкционированный доступ; ● DDoS-атаки **Нарушение защищенности информации:** ● попытки проникновения или прерывания облачных услуг; ● идентификация вредоносных источников данных (PaaS и IaaS) **Эксплуатационные проблемы:** ● проблемы с методами реального анализа (SaaS и PaaS); ●блокировка поставщика услуг (SaaS и PaaS) **Неправильное управление данными:** ● долгосрочность хранения данных (SaaS и PaaS)

мощностей имеющегося аппаратного обеспечения, информационную модель будем считать концептуальной на данном этапе.

Представим облако как объект исследования, где необходимо выделить его компоненты и сопоставить их с соответствующими рисками. Такой подход позволит лучше понять, какие задачи должны быть решены при построении модели безопасной облачной системы.

С архитектурной точки зрения облако можно рассматривать как трехуровневую систему, состоящую из внутреннего (управление ИТ-ресурсами), промежуточного (предоставление ИТ-сервисов) и внешнего (управление приложениями) уровней (рис. 2) [7].

На рис. 2 можно заметить, что каждый уровень облака состоит из взаимосвязанных между собой компонентов. Часть из них уже отвечает за работу с ИБ при запросе пользователя на получение необходимых ему данных из облака, однако не все компоненты являются полностью безопасными. Так, в качестве «менеджера услуг» и «менеджера ИТ-ресурсов» могут выступать как человек (клиент, в случае с IaaS), так и автоматизированная система, откуда возникают риски категории общих проблем безопасности, независимо от того, какая используется модель обслуживания облачных услуг.

Другой пример возможных проблем в части ИБ — система мониторинга. Из-за ее неоднородности может снизиться уровень контроля и надежности ИТ-инфраструктуры и приложений, что влечет за собой увеличение срока устранения возникающих проблем в системе.

Прежде всего, для любой организации при построении безопасной ИТ-инфраструктуры основой является триада сервисов (КЦД):

● конфиденциальность — гарантия того, что информация может быть прочитана и проинтерпретирована только теми людьми и процессами, которые авторизованы для этого;

● целостность — гарантия того, что информация остается неизменной, корректной и аутентичной;

● доступность — авторизованные пользователи могут иметь доступ и работать с информационными активами, ресурсами и системами, которые им необходимы, в нужное им время и с нужной производительностью.

Это является фундаментом ИБ, а для реализации сервисов необходимо внедрение в КИС средств шифрования и технологии ААА (аутентификации, авторизации, аудита и администрирования), которая обеспечит контроль обмена информацией между внешним и промежуточным уровнями облака, куда входят: вход пользователей в систему, проверка их полномочий и прав доступа, а также ведение журналов о потребляемых облачных ресурсах и фактах получения к ним доступа в системе.

Воспользуемся шаблонами «базовая классификация информационных рисков» (Risk classification base sheet) (рис. 3) и «характеристики рисков» (Risk specification sheet), представленными в [6].

Учитывая спецификацию каждой модели обслуживания относительно архитектуры облака (уровней и их компонент), разумно будет добавить еще один тип рисков в шаблон «базовая классификация информаци-

Рис. 2. Архитектура облака

		Идентификатор/Категория	Угроза
Тип риска	Субъективный	Л.1. Нарушение защищенности информации	Перехват, подделка и изменение информационных активов
			.....
		Л.2.....	.....
			.....
	Технический	Т.1. Неправильное управление данными	Недостаточная осведомленность о функциях облачного сервиса
			.....
		Т.2.....	.....
			.....

Рис. 3. Шаблон «базовая классификация информационных рисков»

онных рисков», которую назовем «по модели обслуживания», и соответствующий ему идентификатор «МО».

Окончательно модель информационной системы на основе облака можно представить в обобщенном виде на рис. 4.

Здесь облако рассматривается в общем виде для любой модели SPI. Второй аспект модели — область охвата облачных сервисов на структуре облака, т.е. за какие уровни и компоненты отвечает данная модель обслуживания и на какие информационные риски необходимо обратить внимание при ее использовании. Третий аспект: идентификаторы рисков для каждого из уровней структуры облака и моделей SPI, указанные в соответствии с «Risk classification base sheet» и «Risk specification sheet».

Для выявления наиболее загруженных и вероятных к риску областей структуры облака представим модель в виде неориентированного графа:

$$\text{Cloud} = (\text{Lvls}, \text{Proc}),$$

где вершины графа Lvls — уровни структуры облака, являющиеся элементами объединения множеств, $\text{Lvls} = \text{Exter} \cup \text{Mid} \cup \text{Inter}$.

Здесь элементы каждого множества $\text{Exter} = \{a_1, a_2\}$; $\text{Mid} = \{b_1, b_2, b_3, b_4, b_5\}$; $\text{Inter} = \{c_1, c_2, c_3\}$ обозначают соответсвующие им компоненты уровня (a_1 — портал услуг). Ребра множества $\text{Proc} = \{P_{ij}\}$ — это двусторонние процессы, происходящие с момента запроса услуги.

Опираясь на связи компонентов облака (см. рис. 2), можно построить матрицу смежности и, соответсвенно, сам граф (рис. 5):

Последовательность степеней вершин графа имеет вид $(4, 4, 4, 4, 3, 3, 2, 2, 1, 1) = (a_2, b_2, b_5, c_1, b_4, c_2, a_1, b_1, b_3, c_3)$. Таким образом, возвращаясь к структуре облака, информационные риски на внешнем уровне могут возникнать уже в самом начале процессов, связанных с выбором услуги и ее дальнейшего использования, не

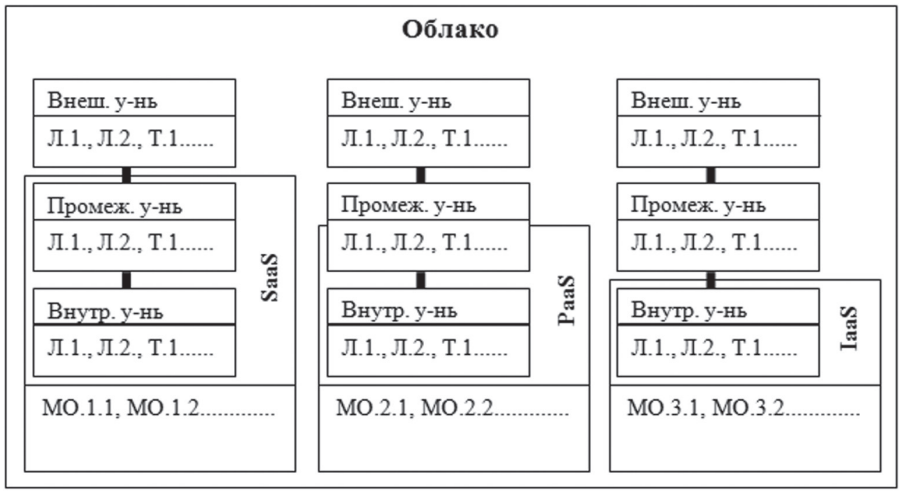

Рис. 4. Обобщенная модель информационной системы на основе облака

	a_1	a_2	b_1	b_2	b_3	b_4	b_5	c_1	c_2	c_3
a_1	0	1	0	0	0	0	1	0	0	0
a_2	1	0	1	1	1	0	0	0	0	0
b_1	0	1	0	0	0	0	0	1	0	0
b_2	0	1	0	0	0	1	1	1	0	0
b_3	0	1	0	0	0	0	0	0	0	0
b_4	0	0	0	1	0	0	1	0	1	0
b_5	1	0	0	1	0	1	0	1	0	0
c_1	0	0	1	1	0	0	1	0	1	0
c_2	0	0	0	0	0	1	0	1	0	1
c_3	0	0	0	0	0	0	0	0	1	0

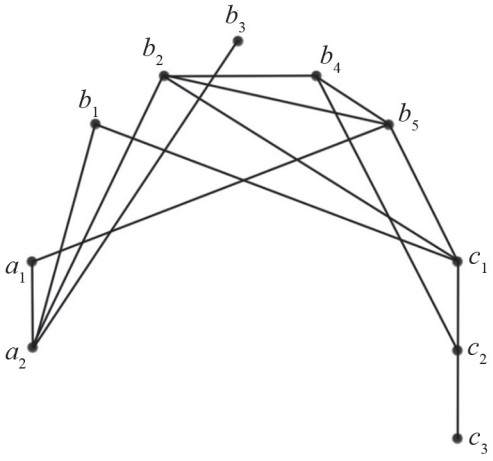

Рис. 5. Неориентированный граф со структурой облака

говоря уже о следующем риск-компоненте базы данных управления конфигурацией (CMDB) промежуточного уровня, который напрямую связан с ними.

Заключение

Основной задачей данной работы стало создание модели безопасной ИС, нацеленной на изучение и выявление рисков ИБ, а также принятие мер по обеспечению безопасности информации при работе с облачными сервисами.

Модель в представленном виде можно использовать как основу для дальнейших исследований и работ по анализу рисков ИБ, присущих облачным вычислениям. Она рассчитана на совместное использование с данными о классификации информационных рисков и их характеристик.

Ее качество будет в дальнейшем проверено при анализе защищенности существующих КИС, использующих облачные сервисы, а также при разработке информационной системы учебного назначения с применением облачных технологий.

Литература

1. **Цыдулко Д.** Рынок облачных технологий: прогнозы на 2017 год [Электрон. ресурс] https://www.crn.ru/ (дата обращения 31.01.2017).

2. **Tadviser.** Ключевые игроки рынка облачных сервисов в России [Электрон. ресурс] http://www.tadviser.ru/ (дата обращения 31.05.2017).

3. **SAPNews.** SAP и Forrester: в России к 2020 году объем «облаков» составит 48 млрд руб [Электрон. ресурс] https://news.sap.com/cis/2017/02/21/ (дата обращения 21.02.2017).

4. **Сот Д.** Oracle CEO Mark Hurd Lays Out the Future of the Cloud [Электрон. ресурс] https://www.oracle.com/corporate/features/openworld-mark-hurd-keynote-2015.html (дата обращения 26.10.2015).

5. **АОБ.** Security Guidance for Critical Areas of Focus In Cloud Computing [Электрон. ресурс] https://cloudsecurityalliance.org/ (дата обращения 26.10.2015).

6. **Нгуен Т.М., Хорев П.Б.** Анализ информационных рисков при использовании облачных вычислений // Информационные системы и технологии. 2017. № 5 (103) С. 117—124.

7. **НОУ Интуит.** Архитектура, принципы и возможности облачных вычислений на платформе Microsoft Azure и ее связь с VisualStudio [Электрон. ресурс] http://www.intuit.ru/ (дата обращения 21.02.2017).

References

1. **Tsydulko D.** Rynok Oblachnykh Tekhnologiy: Prognozy na 2017 God [Elektron. Resurs] https://www.crn.ru/ (Data Obrashcheniya 31.01.2017). (in Russian).

2. **Tadviser.** Klyuchevye Igroki Rynka Oblachnykh Servisov v Rossii [Elektron. Resurs] http://www.tadviser.ru/ (Data Obrashcheniya 31.05.2017). (in Russian).

3. **SAPNews.** SAP i Forrester: v Rossii k 2020 godu Ob"em «Oblakov» Sostavit 48 mlrd rub [Elektron. Resurs] https://news.sap.com/cis/2017/02/21/ (Data Obrashcheniya 21.02.2017). (in Russian).

4. **Sot D.** Oracle CEO Mark Hurd Lays Out the Future of the Cloud [Elektron. Resurs] https://www.oracle.com/corporate/features/openworld-mark-hurd-keynote-2015.html (Data Obrashcheniya 26.10.2015).

5. **AOB.** Security Guidance for Critical Areas of Focus In Cloud Computing [Elektron. Resurs] https://cloudsecurityalliance.org/ (Data Obrashcheniya 26.10.2015).

6. **Nguen T.M., Khorev P.B.** Analiz Informatsionnykh Riskov pri Ispol'zovanii Oblachnykh Vychisleniy. Informatsionnye Sistemy i Tekhnologii. 2017;5 (103):117—124. (in Russian).

7. **NOU Intuit.** Arkhitektura, Printsipy i Vozmozhnosti Oblachnykh Vychisleniy na Platforme Microsoft Azure i ee Svyaz' s VisualStudio [Elektron. Resurs] http://www.intuit.ru/ (Data Obrashcheniya 21.02.2017). (in Russian).

Сведения об авторах

Нгуен Минь Туан — аспирант кафедры прикладной математики НИУ «МЭИ», e-mail: mikikunmiki@gmail.com
Хорев Павел Борисович — кандидат технических наук, профессор кафедры прикладной математики НИУ «МЭИ», e-mail: pbkh@yandex.ru

Information about authors

Nguyen Minh Tuan — Ph.D-student of Applied Mathematics Dept., NRU MPEI, e-mail: mikikunmiki@gmail.com
Khorev Pavel B. — Ph.D. (Techn.), Professor of Applied Mathematics Dept., NRU MPEI, e-mail: pbkh@yandex.ru

Статья поступила в редакцию 13.06.2017