УДК 004.8
doi 10.18101/978–5–9793–0803–6–234–238

МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНОЙ СИСТЕМЫ

© ***Макшанова Лариса Михайловна***, кандидат технических наук,
начальник отдела по работе с операторами связи БФ ОАО «Ростелеком»
Россия, г.Улан-Удэ
E-mail: Larisa.M.Makshanova@sibir.rt.ru

© ***Содномова Марина Станиславовна***, инженер группы ЭКП ОАО МТС
в Республике Бурятия, г.Улан-Удэ, Россия
E-mail: sodnomova86@gmail.com

В данной статье приведена модель угроз информационной безопасности облачных систем. Сложность ее разработки обусловлена виртуализацией вычислительных систем, использованием сети Интернет для доступа к облачным технологиям, а также цепочкой внутренних и внешних поставщиков услуг. Для верной оценки и обеспечения информационной безопасности модель должна учитывать все существующие угрозы и уязвимости. Для этого в статье рассмотрены рекомендации МСЭ-Т X.800, X.805. В последней подробно расписана архитектура сквозной сетевой защиты, которая позволяет учесть угрозы и уязвимости на всем пути реализации информационной системы, поэтому авторы взяли ее за основу построения своей модели. Предложенная в статье модель информационной безопасности облачной структуры учитывает такие особенности, как методы реализации облачной системы, архитектурное построение, а также особенности виртуализации обработки данных.
Ключевые слова: облачная система, облачные решения, информационная безопасность, угрозы, уязвимости.

MODEL OF INFORMATION SECURITY THREATS CLOUD SYSTEM

Larisa M. Makshanova, Candidate of Engineering Sciences,
Head of Department on Work with Operators BF JSC "Rostelecom", Russia, Ulan-Ude

Marina S. Sodnomova, Engineer of the RPC group of MTS OJSC
in the Republic of Buryatia, Russia, Ulan-Ude

This article describes the model of information security threats cloud. The complexity is due to the development of virtualization of computing systems, using the Internet to access the cloud technologies, as well as a chain of internal and external service providers. For the correct evaluation and information security the threat model must take into account all the existing threats and vulnerabilities. For this purpose in the article the ITU-T Recommendation X.800, X.805. ITU-T Recommendation X.805 describes in detail the architecture of the through net protection, which allows you to take into account the threats and vulnerabilities all the way to the implementation of the informational system, so the authors have taken it as the basis for constructing their model. The proposed in the article the Model of informational security of a cloud structure provides the following peculiarities as methods of implement-

tation of cloud systems, architectural building, and also such features as data virtualization.
Keywords: cloud system, cloud solutions, informational security, threats, vulnerability.

Облачные технологии (Cloud Computing) — это технологии распределенной обработки данных, в которых информационные ресурсы и мощности предоставляются потребителю как сервис посредством Интернет. По способам и методам реализации облачной системы разделяют на [1]:

✓ **Частное облако** (англ. *private cloud*) — инфраструктура, предназначенная для использования одной организацией, включающей несколько потребителей (например, подразделений одной организации), возможно также клиентами и подрядчиками данной организации. Частное облако может находиться в собственности, управлении и эксплуатации как самой организации, так и третьей стороны (или какой-либо их комбинации), и оно может физически существовать как внутри, так и вне юрисдикции владельца.

✓ **Публичное облако** (англ. *public cloud*) — инфраструктура, предназначенная для свободного использования широкой публикой. Публичное облако может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций (или какой-либо их комбинации). Публичное облако физически существует в юрисдикции владельца — поставщика услуг.

✓ **Общественное облако** (англ. *community cloud*) — вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи (например, миссии, требований безопасности, политики и соответствия различным требованиям). Общественное облако может находиться в кооперативной (совместной) собственности, управлении и эксплуатации одной или более организаций сообщества или третьей стороны (или какой-либо их комбинации), и оно может физически существовать как внутри, так и вне юрисдикции владельца.

✓ **Гибридное облако** (англ. *hybrid cloud*) — это комбинация из двух или более различных облачных инфраструктур (частных, публичных или общественных), остающихся уникальными объектами, но связанных между собой стандартизованными или частными технологиями передачи данных и приложений (например, кратковременное использование ресурсов публичных облаков для балансировки нагрузки между облаками).

Рассмотренные реализации облачных технологий позволяют предоставлять широкий спектр услуг населению и коммерческим предприятиям. Гибкость и легкость масштабирования необходимых процессорных и программных мощностей облачных технологий позволяют минимизировать CAPex– и OPex-расходы на покупку, содержание, обслуживание и оптимизацию ИТ-инфраструктуры, ПО и обслуживающего персонала. В свою очередь все услуги на основе облачных технологий разделяют на [2]:

✓ IaaS (Infrastructure as a Service или «Инфраструктура как сервис») — компьютерная инфраструктура, как правило, представленная в форме виртуализации. Является услугой в рамках концепции облачной обработки данных.

✓ PaaS (Platform as a Service или «Платформа как сервис») — интегрированная платформа для разработки, развертывания, тестирования и поддержки web-приложений. Представлена в виде сервиса на основе концепции «облачные вычисления».

✓ SaaS (Software as a service или «ПО как сервис») — представляет собой бизнес-модель лицензионного использования ПО, которая подразумевает разработку и поддержку программного обеспечения поставщиком. Заказчикам же предоставляется возможность его платного использования, как правило, посредством Интернета.

✓ DaaS (Desktop as a Service или «Рабочий стол как сервис») — еще одна бизнес-модель лицензионного использования программного обеспечения, которая представляет собой немного усовершенствованную модель SaaS, в основном предполагающая использование нескольких сервисов одновременно, необходимых для полноценной работы. Впервые была представлена в начале 2000-х годов.

Виртуализация вычислительных систем, использование сети Интернет для доступа к облачным технологиям, цепочка внутренних и внешних поставщиков услуг расширяют задачи обеспечения информационной безопасности на физическом и сетевом уровнях, к ним также прибавляются проблемы регулировки и выполнения стандартов потребителей (предприятий, банков и т. д.) в области хранения данных.

Согласно определениям Рекомендации X.800, угроза безопасности — это потенциальное нарушение безопасности. Уязвимость — это результат ошибки или дефекта, которыми можно воспользоваться с целью нарушения системы или содержащейся в ней информации. Уязвимости бывают 4 видов: уязвимость, обусловленная проектом и техническими характеристиками; уязвимость реализации; уязвимость эксплуатации и реализации; уязвимость, зависящая от модели угроз. Риск — это показатель негативных последствий, которые могут произойти, если воспользоваться уязвимостью, т.е реализация угрозы. Таким образом, правильная оценка уязвимостей и угроз позволяет минимизировать риски и принять проактивные меры для информационной защиты системы.

Согласно рекомендации X.805 «Безопасность в электросвязи и информационных технологиях», архитектура сквозной сетевой защиты определяется такими понятиями, как слои (слой инфраструктуры, слой услуг и слой приложений) и плоскости безопасности (плоскость административного управления, плоскость оперативного управления и плоскость конечного пользователя). Наряду с двумя составляющими — слоями безопасности и плоскостями безопасности — в рамках структуры определены также восемь параметров безопасности: секретность, конфиденциальность, аутентификация, целост-

ность, сохранность информации, управление доступом, безопасность связи и готовность.

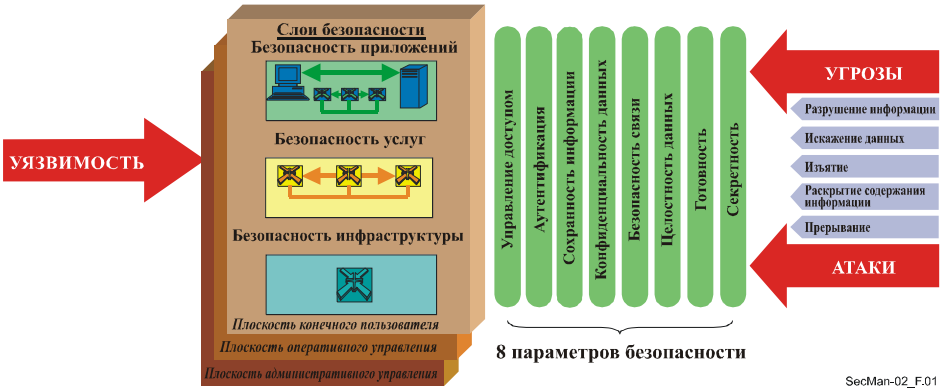

Рис. 1. Элементы архитектуры безопасности согласно Рек. МСЭ-Т X.805 [4]

Для обеспечения ИБ облачной системы необходимо верно оценить существующие уязвимости, угрозы и существующие риски. На рис. 2 представлена модель угроз, учитывающая каждый уровень ее архитектурной реализации:

- ✓ Аппаратная часть;
- ✓ Гипервизор — системное ПО виртуализации, управляющее аппаратными ресурсами и ресурсами виртуальных машин;
- ✓ Система управления виртуальной средой;
- ✓ Инфраструктура виртуальных машин;
- ✓ Сеть хранения данных — включает в себя коммутационное оборудование и СУБД, с размещенными образами виртуальных машин и данными.

Приведенная модель угроз облачной системы позволяет структурировать и классифицировать угрозы, связанные с виртуализацией вычислительных систем. Для каждой идентифицированной угрозы необходимо составить список уязвимостей в отношении 8 параметров безопасности согласно Рек. X805, что обусловлено особенностями обработки данных в виртуальной среде:

- ✓ Обработка данных совершается на виртуальных машинах, которые могут быть реализованы на разных серверах, а сами серверы могут принадлежать различным информационным системам персональных данных;
- ✓ Передача данных между виртуальными машинами осуществляется по виртуальной среде, то есть данные проходят через цепочку коммутационного оборудования из одной виртуальной среды в другую;
- ✓ Передача данных также осуществляется между виртуальной и внешней средой.

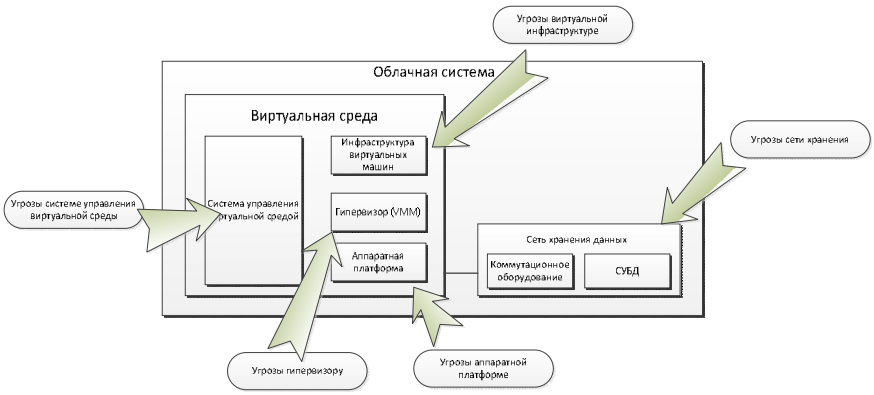

Рис. 2. Модель ИБ угроз облачной системы

Выводы. В статье приведена модель угроз ИБ облачной системы и дана оценка уязвимостей, связанных с особенностями обработки данных в виртуальной среде.

Литература

1. URL: http://www.tadviser.ru/index.php / Статья /:Публичные_облака_vs_ Частные_облака
2. URL: http://skyblogger.net/2013/04/16/bezopasnost-oblachnyh-tehnologiy. html.
3. Рекомендация X.800 МСЭ-Т «Архитектура безопасности для взаимосвязи открытых систем».
4. Рекомендация X.805 МСЭ-Т «Безопасность в электросвязи и информационных технологиях».
5. URL: http://www.slideshare.net/SoftlineCompany/softline-13753827? related=3