*A. V. Tsaregorodtsev, E. V. Makarenko*

**Vulnerability Assessment for Various Types of Cloud Structures**

*Keywords: cloud computing, information security threats, attack, damage, system vulnerability assessment, factor counteracting*

Today organizations increasingly consider cloud computing as an alternative way of using information technology. At the same time, the use of different vulnerabilities of infrastructure components, network services and applications remains are the major threat to the cloud. The article proposes a methodology for vulnerability assessment for any type of cloud structures, which will allow to determine the coefficient of counter to possible attacks and to correlate the amount of damage to the total cost of ownership of organization IT-infrastructure.

*А. В. Царегородцев, Е. В. Макаренко*

# ОЦЕНКА УЯЗВИМОСТЕЙ ДЛЯ РАЗЛИЧНЫХ ТИПОВ РАЗВЕРТЫВАНИЯ ОБЛАЧНЫХ СРЕД

## Введение

Практически все технологии, которые сегодня входят в состав облачной парадигмы, существовали и раньше, однако до настоящего времени на рынке не было предложений, которые объединяли бы перспективные технологии в едином коммерчески привлекательном решении. И только в последнее десятилетие появились облачные сервисы, благодаря которым эти технологии стали, с одной стороны, доступны разработчику, а с другой — понятны для бизнес-сообщества [1].

Облачные вычисления экономически эффективны с точки зрения совокупной стоимости владения, что позволяет сократить стоимость технического обслуживания. Большая часть годовых бюджетов в большинстве ИТ-подразделений идет на обслуживание и амортизацию инфраструктуры, не предоставляя при этом новой добавленной стоимости.

Тем не менее облачные вычисления — это новая форма распределенных вычислений, которая все еще находится в зачаточном состоянии. Используя парадигму облачных вычислений, организация отказывается от прямого контроля над многими аспектами безопасности и, тем самым, создает беспрецедентный уровень доверия облачному провайдеру, что может иметь далеко идущие планы для разработки систем федеральных агентств, образовательных учреждений и других государственных организаций [2]. Но многие из функций, которые делают привлекательными облачные вычисления, могут вступать в противоречие с традиционными моделями обеспечения информационной безопасности.

Возможность использования различных уязвимостей компонентов инфраструктуры, сетевых сервисов и приложений остается главной угрозой для облачных сервисов [3]. Данный аспект представляет серьезную опасность для общедоступных PaaS- и IaaS-моделей, в которых управление уязвимостями, конфигурацией и обновлением находится в зоне ответственности облачного клиента. В общественной облачной среде (OOC) общий уровень защищенности распределен между участниками всей многопользовательской виртуальной среды. С одной стороны, ответственность за управление уязвимостями, обновлением и конфигурацией (VPC) инфраструктуры лежит на провайдере, с другой — клиенты облачной среды должны понимать именно те аспекты VPC, за которые они ответственны.

Рассмотрим особенности управления уязвимостями, обновлением и конфигурацией в разрезе моделей предоставления сервисов и зон ответственностей между провайдером и клиентом.

### 1. Управление уязвимостями, конфигурацией и обновлениями

Управление уязвимостями — важный элемент сдерживания возможных угроз с целью защиты хоста, сетевых устройств и приложения от атак (рис. 1). Организации, которые заботятся об обеспечении информационной безопасности, вводят процедуры управления уязвимостями, которые включают в себя стандартное сканирование систем, подключенных к сети, анализ рисков возникновения уязвимостей и модификацию процесса для устранения рисков. Организации, принимая во внимание стандарт ISO/IEC 27002, используют технические возможности по управлению уязвимостями, которые основываются на принципе достижения приемлемого риска, возникающего при эксплуатации. Управление уязвимостями должно быть реализовано в виде эффективной и систематической процедуры с возможностью измерения ее эффективности.

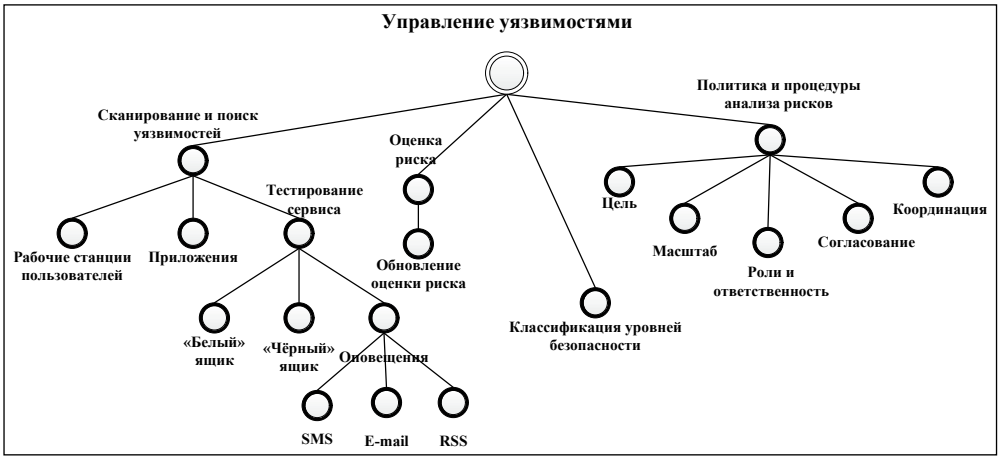


*Рис. 1. Дерево целей управления уязвимостями среды облачных вычислений*

Аналогично управлению уязвимостями, управление обновлениями и исправлениями является важным элементом сдерживания возможных угроз на уровне хоста, сетевых устройств и приложений, где действия неавторизованных пользователей направлены на использование известных им уязвимостей.

SaaS-провайдеры должны оценивать новые уязвимости и исправлять аппаратное и программное обеспечение на всех системах, которые предназначены для поставки клиентам. Клиенты полностью освобождены от процедур обновления в среде SaaS, но при этом ответственны за управление патчами для целого стека программного обеспечения (ОС, приложения, базы данных), установленного и управляемого на платформе IaaS. Клиенты также несут полную ответственность за исправление приложений, развернутых на платформе PaaS.

Управление конфигурацией безопасности является еще одним важным аспектом в управлении угрозами для сетевых устройств и узлов от неавторизированных пользователей, использующих любые «узкие места» в конфигурации (рис. 2). Защита конфигурации сети, узла и приложения влечет за собой контроль и управление доступом к критически важной системе и базе данных конфигурационных файлов, в том числе конфигурации ОС, политике брандмауэра, сетевым настройкам зоны локального и удаленного хранения данных и управления базами данных.

Провайдеры сервисов SaaS и PaaS несут полную ответственность за управление конфигурацией своих платформ, а клиенты IaaS несут ответственность за управление конфигурацией ОС, приложений и баз данных.

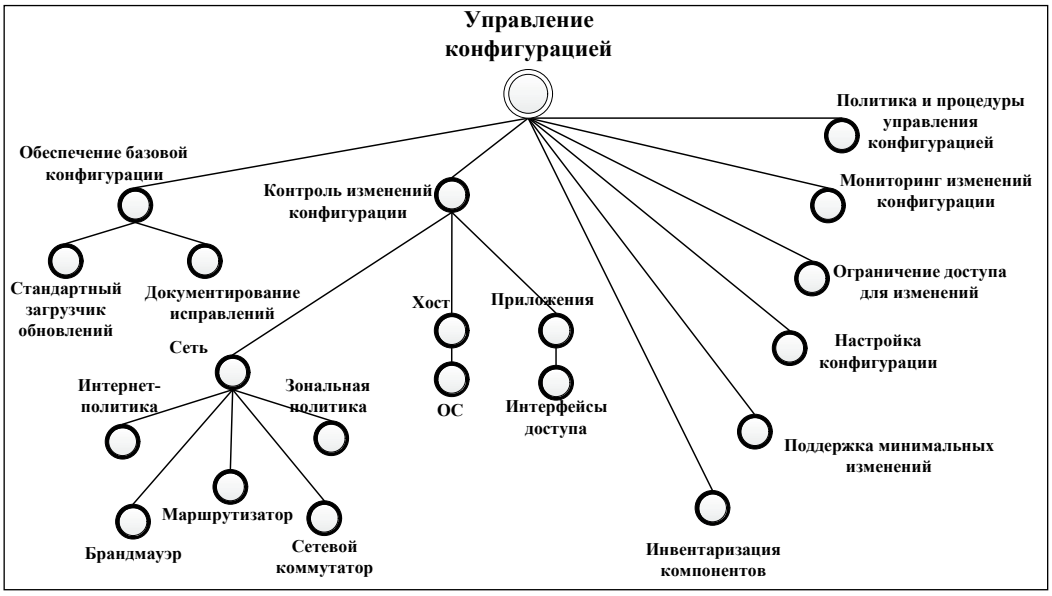


*Рис. 2. Дерево целей управления конфигурацией среды облачных вычислений*

## 2. Анализ результатов оценки уязвимостей для различных типов развертывания облачных сред

Используя данные статистик по основным уязвимостям среды облачных вычислений, рассчитаем уровень защищенности каждой отдельной инфраструктуры по методике «NVD Common Vulnerability Scoring System Support v.2» Национального института стандартов и технологий США [4].

Общая система оценки уязвимостей (CVSS) обеспечивает открытую архитектуру для получения взаимосвязей, особенностей и влияний уязвимостей на рассматриваемую ИТ-инфраструктуру. Методика CVSS включает расчеты по 3 группам: базовой группе, временной группе, факторам окружающей среды.

Результатом расчетов для каждой группы являются числовая оценка в диапазоне от 0 до 10 и вектор, содержащий сжатое текстовое описание для полученных значений. Базовая группа представляет внутренние характеристики возможных уязвимостей. Временная группа отражает характеристики уязвимостей, которые изменяются с течением времени. Группа факторов окружающей среды представляет характеристики уязвимостей, которые являются уникальными для различных сред. Инструментарий CVSS позволяет получить оценку ИТ-уязвимостей различного характера, в том числе для разных типов развертывания облачных сред. На рис. 3 изображен набор метрик CVSS.

Результат проведения оценки на уязвимости по методике CVSS для частной облачной среды (ЧОС), ООС и гибридной облачной среды (ГОС) представлен в таблице 1.

Полученные результаты оценок возможных уязвимостей для различных типов развертывания облачных сред показывают, что использование общественного облака неприемлемо в случае обработки критичных данных, а золотой серединой является вариант гибридной облачной среды.

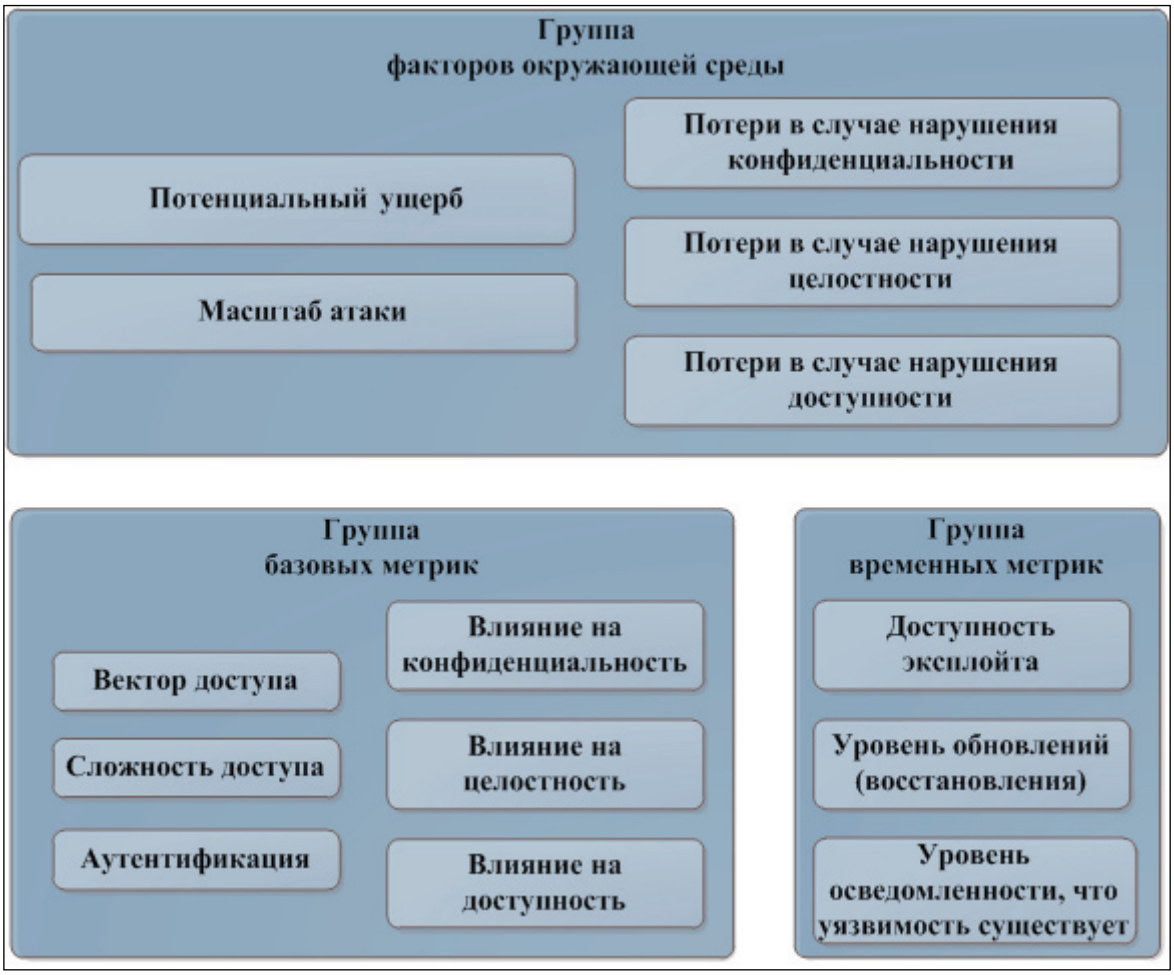


*Рис. 3. Набор метрик CVSS*

*Таблица 1. Оценка на уязвимости по методике CVSS*

| | ООС | ЧОС | ГОС |
|---|---|---|---|
| 1. **Группа базовых метрик** | 9 | 3,4 | 7 |
| 1.1. Вектор доступа | Общедоступная сеть | Локальная сеть | Гибридная сеть |
| 1.2. Сложность доступа | Низкая | Высокая | Средняя |
| 1.3. Аутентификация | Однофакторная | Многофакторная | Многофакторная |
| 1.4. Влияние на конфиденциальность | Полное | Частичное | Полное |
| 1.5. Влияние на целостность | Полное | Частичное | Полное |
| 1.6. Влияние на доступность | Полное | Частичное | Полное |
| 2. **Группа временных метрик** | 6,2 | 3,6 | 6 |

| | | | |
|---|---|---|---|
| 2.1. Доступность для эксплойтов | Высокая | Функциональная | Функциональная |
| 2.2. Уровень обновлений (восстановления) | Официальные исправления (патч) | «Заплатка» | Временное решение |
| 2.3. Уровень осведомленности, что уязвимость существует | Подтвержденный | Неподтвержденный | Подтвержденный |
| 3. **Группа метрик окружающей среды** | 6,1 | 1,5 | 2 |
| 3.1. Потенциальный ущерб | Высокий (катастрофические потери) | Высокий (катастрофические потери) | Высокий (катастрофические потери) |
| 1.2. Масштаб атаки | Высокий (26–75 % активов в зоне риска) | Низкий (0–25 % активов в зоне риска) | Низкий (0–25 % активов в зоне риска) |
| 3.3. Потери в случае утери конфиденциальности | Высокие | Высокие | Высокие |
| 3.4. Потери в случае утери целостности | Высокие | Высокие | Высокие |
| 3.5. Потери в случае утери доступности | Высокие | Высокие | Высокие |
| **Общая оценка CVSS** | **6,7** | **1,5** | **2** |

Интерпретируем полученные результаты оценки уязвимостей в коэффициент противодействия различному виду угроз, исходя из соотношения, что CVSS-оценка, равная 1,5, соответствует 85 % эффективности защиты облачной ИТ-инфраструктуры (таблица 2).

*Таблица 2. Коэффициент противодействия для вариантов облачных сред*

| Вариант | Общая оценка CVSS | Коэффициент противодействия |
|---|---|---|
| ЧОС | 1,5 | **85 %** |
| ГОС | 2 | **80 %** |
| ООС | 6,7 | **33 %** |

В таблице 3 отражены результаты применения механизмов защиты в различных облачных средах на примере стоимости инцидента «Кража конфиденциальной информации, к которой не был предусмотрен доступ по политике безопасности, недобросовестным сотрудником (используя привилегии)» = 5 283 168,00 р.

*Таблица 3. Коэффициент противодействия для вариантов облачных сред*

| Вариант облачной архитектуры | Эффективность защиты конфиденциальных данных | Сумма сохраненных средств за 1 год | Величина ущерба |
|---|---|---|---|
| ЧОС | **85 %** | 4 490 692,80 р. | 792 475,20 р. |
| ГОС | **80 %** | 4 226 534,40 р. | 1 056 633,60 р. |
| ООС | **33 %** | 1 743 445,44 р. | 3 539 722,56 р. |

Проведенная экспериментальная оценка эффективности защиты конфиденциальных данных подтвердила необходимость применения дополнительных методик защиты информации в рассматриваемых примерах для построения облачной среды.

**Заключение**

На основе общей системы оценки уязвимостей, позволяющей определить качественный показатель подверженности уязвимостям информационных систем с учетом факторов окружающей среды, предложена методика по оценке возможных уязвимостей для различных типов развертывания облачных сред.

Применение методики по оценке уязвимостей для различных типов развертывания облачных сред позволило выявить коэффициент противодействия возможным атакам и соотнести величину ущерба с совокупной стоимостью владения всей ИТ-инфраструктуры организации.

## СПИСОК ЛИТЕРАТУРЫ:

1. *Качко А. К., Лавриненко М. М., Царегородцев А. В.* Один из подходов к построению гибридной защищенной облачной среды // Безопасность информационных технологий. 2014. № 1. С. 22–27.
2. *Maches B.* The Impact of cloud computing on corporate IT governance. HBCWire.com. [Электронный ресурс]. URL: http://www.hpcwire.com/specialfeatures/cloud_computing/features/The-Impact-of-Cloud-Computing-on-Corporate-IT-Governance-82623252.html (дата обращения: 28.08.2014).
3. *Царегородцев А. В.* Анализ рисков безопасности данных в корпоративных сетях кредитно-финансовых организаций на основе облачных вычислений // Национальные интересы: приоритеты и безопасность. 2013. № 39 (228). С. 35–44.
4. NVD Common Vulnerability Scoring System Support v.2. Национальный институт стандартов и технологий США. [Электронный ресурс]. URL: http://nvd.nist.gov/cvss.cfm?calculator&version=2 (дата обращения: 28.08.2014).

## REFERENCES:

1. *Kachko A. K., Lavrynenko M. M., Tsaregorodtsev A. V.* The approach of secure hybrid cloud construction // Safety of information technology. 2014. № 1. P. 22–27.
2. *Maches B.* The Impact of cloud computing on corporate IT governance. HBCWire.com. [Electronic resource].
URL: http://www.hpcwire.com/specialfeatures/cloud_computing/features/The-Impact-of-Cloud-Computing-on-Corporate-IT-Governance-82623252.html (date of access: 28.08.2014).
3. *Tsaregorodtsev A. V.* Data safety risk analysis in credit-financial corporative networks on the basis of cloud computing // National interests: priorities and safety. 2013. № 39 (228). P. 35–44.
4. NVD Common Vulnerability Scoring System Support v.2. The National Institute of Standards and Technology, USA. [Electronic resource]. URL: http://nvd.nist.gov/cvss.cfm?calculator&version=2 (date of access: 28.08.2014).