УДК 004.056:061.68

А.В. Царегородцев, А.Н. Зеленина, В.А. Савельев

КЛАССИФИКАЦИЯ УЯЗВИМОСТЕЙ ОБЛАЧНЫХ СРЕД В ЗАДАЧЕ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ РИСКА

Московский государственный лингвистический университет, Москва, Россия
Воронежский институт высоких технологий, Воронеж, Россия

Практически все технологии, которые сегодня входят в состав облачной парадигмы, существовали и раньше, однако до настоящего времени на рынке не было предложений, которые бы объединяли перспективные технологии в едином коммерчески привлекательном решении. И только в последнее десятилетие появились общедоступные облачные сервисы, благодаря которым эти технологии стали, с одной стороны, доступны разработчику, а с другой – понятны для бизнес-сообщества. Но многие из функций, которые делают привлекательными облачные вычисления, могут вступать в противоречие с традиционными моделями обеспечения информационной безопасности. На основе общей системы оценки уязвимостей, позволяющей определить качественный показатель подверженности уязвимостям информационных систем с учетом факторов окружающей среды, предложена методика по оценке рисков для различных типов развёртывания облачных сред. На основе широко используемой Общей системы учета уязвимостей, которая помогает определить качественный показатель подверженности уязвимостям информационных систем, в статье предлагается классификация уязвимостей, характерных для различных типов развертывания облачных сред.

Ключевые слова: информационная безопасность, облачные вычисления, уязвимости, риск модель, оценка риска.

Введение

Актуальной научной задачей является классификация уязвимости облачных сред и анализ возможности использования этой информации при проведении количественной оценки риска.

Одной из серьезных угроз информационной безопасности (ИБ) облачных сред является использование со стороны злоумышленников известных, но не исправленных уязвимостей. Успешная реализация эксплойта потенциально может привести к значительному финансовому ущербу для клиента, потере репутации облачного провайдера и компрометации используемых механизмов защиты [1].

1. Методика оценки рисков ИБ

Обозначим основные понятия, которые будут использованы в методике. Угроза безопасности – это потенциальное нежелательное событие в объекте оценки, которое может привести к успешному использованию эксплойта с нежелательным влиянием на конфиденциальность, целостность, доступность активов объекта оценки.

Заинтересованные лица могут нанести ущерб или вред организации, обнаружив дефект программного обеспечения (ПО) или ненадежность системы. Это и будет означать уязвимость. Известные уязвимости будут определяться как те, которые не имеют патчей с исправлениями, так и те, для которых выпущены патчи, но с задержкой по времени. Злонамеренным использованием [2] назовем появление нежелательного события в результате использования уязвимости некой угрозой. Отметим, что злонамеренные использования могут обнаружиться в случае появления, и угрозы, и уязвимости, и такая уязвимость может быть использована конкретной угрозой (рисунок 1).

Рисунок 1 – Взаимосвязи угроз и уязвимостей

Из рисунка 1 следует, что во множество всех злонамеренных событий входит подмножество уязвимостей и подмножество угроз. Следовательно,

$$M = \subset ST \cap SV,$$

где M – это набор злонамеренных событий,
ST – это множество угроз,
SV – это множество уязвимости.

Представим методику оценки рисков в виде следующих связанных процессов (таблица 1) [3].

Сначала описывается управляемый риском анализ, включающий оценку набора злонамеренного использования и уровня риска, затем

сравниваем полученные значения с критериями принятия риска. Получаем набор рисков, требующих обработки.

Таблица 1 – Методика оценки риска

№	Описание процесса/действия
1	Идентификация контекста оценки риска
1.1	Идентификация цели и масштаба оценки
1.2	Описание объекта цели, бизнес требований и среды безопасности
1.3	Определение владельцев процесса
1.4	Идентификация активов и классификация активов со стороны владельцев
1.5	Описание графа активов и владельцев
1.6	Описание политики безопасности
1.7	Идентификация и описание критериев принятия рисков
2	Идентификация риска
2.1	Идентификация угроз безопасности и влияние на активы
2.2	Идентификация уязвимостей объекта оценки, принципов обеспечения, процессов, процедур и среды безопасности
2.3	Документирование сценариев злонамеренного использования и их группировка
3	Анализ риска
3.1	Оценка уровня влияния злонамеренного использования
3.2	Оценка частоты злонамеренного использования
4	Оценивание риска
4.1	Определение уровня риска для каждого набора частоты и влияния
4.2	Оценивание риска и сравнение с критериями принятия риска
4.3	Категоризация риска для обработки в наборы рисков
4.4	Определение внутренних взаимосвязей между наборами рисков
4.5	Идентификация конфликтов между наборами риска
4.6	Назначение приоритетов наборов и рисков
4.7	Решение найденных конфликтов
5	Обработка риска
5.1	Идентификация альтернативных решений по обеспечению безопасности и группировка их в наборы
5.2	Идентификация эффекта и цели альтернативных систем защиты информации (СЗИ)
5.3	Моделирование СЗИ
5.4	Оценка и поиск оптимальной СЗИ или набора решений по обеспечению безопасности.

Набор рисков для обработки, альтернативных решений, соответствующих проекту, а так же ряд других параметров являются входными данными для второго этапа, в рамках которого определяются решения в виде доступных механизмов безопасности [4, 5].

Описанные действия в рамках первого этапа включают в себя ключевые элементы анализа: набор угроз, уязвимости, злонамеренное использование, его частота и влияние, риск ИБ, критерии принятия риска.

Таким образом, построение риск-модели облачных вычислений выполняется последовательно за счет двух шагов: сначала определяется состояние модели исходя из оценки урона при успешной реализации эксплойта. Затем – состояние модели исходя из оценки частоты применения эксплойта.

На шаге 1 определяется список уязвимостей на основании общедоступных данных, например, из официальных сообщений о уязвимостях или баз данных (NVD).

На шаге 2 исследуется модель переходов состояний, полученная на первом этапе и дополняется интенсивностью переходов.

Интенсивность переходов показывает с какой вероятностью возможен переход из одного состояния в другое и с какой вероятностью возможно нахождение в этом состоянии в определенный интервал временной времени.

Модель переходов состояний описывает различные уровни риска, характерные для рассматриваемой среды в какой-то момент времени. Для определения интенсивности переходов принимается во внимание агрегированная частота использования эксплойта в определенный временной интервал.

2. Классификация уязвимостей среды облачных вычислений на основе CVSS

Общая система учета уязвимостей (CVSS) достаточно широко применяется в настоящее время для определения и оценки уязвимостей.

Главная задача состоит в оценке уровня серьезности, имеющего отношение к уязвимостям, и предоставление рекомендаций по снижению результатов угроз. Можно отметь, что общая система учета уязвимостей представляет собой инструмент для анализа характеристик и влияния уязвимостей, независимо от вендора программного обеспечения, поэтому может быть использована для классификации уязвимостей облачных сред.

На основе CVSS был проанализирован и представлен в виде таблицы 2 список уязвимостей, характерных для технологии облачных вычислений с целью дальнейшего использования этих данных для построения риск модели облачных сред различных типов развертывания.

Таблица 2 – Перечень уязвимостей, характерных для технологии облачных вычислений

№	Название уязвимости	Описание уязвимости

№	Название уязвимости	Описание уязвимости
1.	Уязвимости типа AAA	Слабая система аутентификации, авторизации и учетных данных может облегчить доступ к ресурсам, привести: •к неправомерной эскалации привилегий, •к невозможности отслеживания нецелевого (злонамеренного) использования ресурсов, •к появлению инцидентов из-за: – небезопасного хранения параметров доступа к облачной среде; – недостаточного количества ролей; – хранения учетных данных на временных инстанциях виртуальной машины.
2.	Уязвимости предоставления прав пользователям	•отсутствие контроля над процессом предоставления прав со стороны клиента, •отсутствие идентификации клиентов при осуществлении регистрации, •задержка при синхронизации между компонентами облачной среды профилей пользователей, •совершение множественного несинхронного копирования идентификационных данных.
3.	Уязвимости перераспределения прав пользователям	Отозванные полномочия являются валидными из-за задержек при развертывании на все компоненты облачной среды.
4.	Удаленный доступ к интерфейсу управления	Теоретически позволяет успешно применить эксплойт на конечном устройстве клиента, что нарушит нормальное функционирование системы безопасности облака с помощью слабой аутентификации запросов и ответов.
5.	Уязвимости гипервизора	Уязвимости гипервизора являются самыми критическими, так как гипервизор управляет физическими ресурсами и всеми виртуальными машинами облачной среды.
6.	Отсутствие изоляции ресурсов	Использование ресурсов одного облачного клиента может повлиять на ресурсы другого клиента. IaaS строится по принципу разделения

№	Название уязвимости	Описание уязвимости
		физических ресурсов облака на множество виртуальных машин, которое использует разные клиенты. Уязвимости гипервизора могут привести к неавторизованного доступу к этим коллективно используемым ресурсам.
7.	Отсутствие изоляции репутации	Действия одного облачного клиента могут привести к компрометации данных других клиентов.
8.	Уязвимости шифрования передачи данных (архивов, журналов)	Возможность чтения данных при передаче между компонентами облачной среды с использованием атак типа «человек посередине», слабой аутентификации, самоподписанных сертификатов.
9.	Отсутствие механизмов для оценки уязвимостей	Ограничения со стороны провайдера, отраженные в договоре использования могут сделать невозможным сканирование портов, использование сканеров уязвимостей, что является серьезной проблемой информационной безопасности.
10.	Слабые процедуры управления ключами шифрования	Облачная инфраструктура требует управления и хранения различных наборов ключей: ключи шифрования данных при передаче, ключи шифрования файлов, ключи для идентификации провайдеров, клиентов, ключи для авторизации по токенам. Виртуальные машины не имеют фиксированной аппаратной инфраструктуры и все данные клиента могут быть распределены по распределённым облачным дата центрам, что затрудняет применение стандартных механизмов безопасности, таких как: аппаратные модули безопасности (HSM). •интерфейс управления ключами, доступный по Интернет соединению, является более уязвимым по сравнению с традиционными вариантами развертывания ИТКС, •новые виртуальные машины для возможности проведения аутентификации должны разворачиваться с требуемым уровнем

№	Название уязвимости	Описание уязвимости
		параметров безопасности. Распространение этих параметров может быть затруднительно из-за эффекта масштаба, так как при незапланированном увеличении мощности, подключении большого количества виртуальных машин потребуется время: – для регистрации сертификатов; – для аутентификации новых компонентов и распространении новых данных для установления подлинности, • аннулирование (отмена) ключей для проверки подлинности также является сложной задачей и требует внедрения доп. решений, таких как OCSP.
11.	Генерирование ключей: низкий уровень энтропии при генерации случайных чисел	Злоумышленник, взломав одну из виртуальных машин может подобрать ключи доступна к другим виртуальным машинам по причине использования одного и того же источника энтропии.
12.	Некорректное планирование использования ресурсов	Облачные сервисы особенно уязвимы по причине истощения ресурсов. Многие провайдеры позволяют клиентам резервировать ресурсы предварительно, но планирование может быть затруднено в силу неточного моделирования использования ресурса, что приведет избыточному резервированию со стороны клиента (тем самым приводя к потраченным впустую ресурсам со стороны провайдера облака).
13.	Возможность активной разведки внутренней сети	Облачные клиенты могут проводить сканирование портов, которые используют другие клиенты.
14.	Возможность проведения проверки распределения ресурсов	Атака по сторонним (побочным) каналам используя уязвимости отсутствия изоляции, может привести к ситуации, когда злоумышленник определит какие ресурсы распределены по клиентам.
15.	Отсутствие данных для анализа	Доступность чтения журналов и логов ограничена моделью предоставления облачных сервисов. SaaS провайдеры не предоставляют доступа к логу IP клиентов, обращающихся к облаку. IaaS

№	Название уязвимости	Описание уязвимости
		провайдеры могут не предоставить актуальную информацию о версии образа виртуальной машины и других компонентов облачной среды.
16.	Удаление критически важных данных	Общие физические носители информации могут стать причиной утечки критически важных данных. Для них невозможно применить полноценные процедуры удаления данных, так как физическое уничтожение недопустимо из-за того, что дисковое пространство одновременно используется со стороны других клиентов.
17.	Разделение ответственности и контрактных обязательств. Конфликт интересов клиентов.	Облачные клиенты в общем случае не знают или не исполняют своих обязательство в соответствие с условиями обслуживания. Ряд требований может быть отражено в SLA, например, по шифрованию архивов, однако, никакой ответственности провайдера за нарушение выполнения таких процедур в договоре нет.
18.	Скрытая зависимость при использовании кросс облачных приложений	Скрытая зависимость может проявляться при осуществлении передачи данных в облако и из облака, облачная архитектура может не предусматривать продолжительный траффик из облака.
19.	Невозможность проведения сертификации и аудита	Отсутствие со стороны провайдера гарантий по проведению внутреннего аудита или сертификации. Например, некоторые провайдеры используют гипервизоры с открытым исходным кодом и изменяют его без соблюдения общих критериев оценки безопасности.
20.	Отсутствие механизма для ограничения выделения ресурсов	Нет гибких механизмов для клиента и облачного провайдера для определения порога использования ресурсов. Это может стать проблемой в случае незапланированного использования ресурсов со стороны клиента.

Заключение

Анализ рисков и анализ возможных угроз служат обоснованием выбора комплекса мероприятий обеспечения информационной безопасности в облачных средах. Комплекс мероприятий должен быть осуществлен для снижения риска до приемлемого уровня. Для решения

этой задачи в статье на основе Общей системы учета уязвимостей CVSS представлена классификация уязвимостей облачных сред с целью дальнейшего использования этих данных для построения риск модели облачных сред различных типов развертывания с возможностью использовать эту информацию при проведении оценки количественных показателей риска.

ЛИТЕРАТУРА

1. Царегородцев, А.В. Модель оценки рисков информационной безопасности информационных систем на основе облачных вычислений [Текст] / Царегородцев, А.В., Ермошкин, Г.Н. // Национальная безопасность. 2013. №6(29). С.46-54.
2. Царегородцев, А.В. Оценка уязвимостей для различных типов развертывания облачных сред [Текст] / Царегородцев, А.В., Макаренко, Е.В. // Безопасность информационных технологий. 2014. №4. С.112-117.
3. Царегородцев, А.В. Один из подходов к оценке рисков информационной безопасности в облачных средах [Текст] / Царегородцев, А.В., Малюк, А.А., Макаренко, Е.В. // Безопасность информационных технологий. – М., 2014. – №4. – С.68-74.
4. Tsaregorodtsev, A. Methodology of vulnerability assessment for various types of cloud structures [Текст] / Tsaregorodtsev, A., Zelenina, A., Ružický, E. // Information Technology Applications. – Bratislava, Slovakia, 2017. – №1. – С.51-60.
5. Tsaregorotsev, A. Automation of the distribution process of sensitive data processing in a hybrid cloud computing environment [Текст] / Tsaregorotsev, A., Zelenina A. // Information Technology Applications. – Bratislava, Slovakia, 2016. – №1. – С.137-149.

A.V. Tsaregorodtsev, A.N. Zelenina, V.A. Savelev

VULNERABILITY CLASSIFICATION OF CLOUD TOOLS IN THE PROBLEM OF QUANTITATIVE RISK ASSESSMENT

Moscow State Linguistic University, Moscow, Russia
Voronezh Institute of High Technologies, Voronezh, Russia

Almost all technologies that are now part of the cloud paradigm existed before, but so far there have been no offers on the market that would combine the promising technologies in a

single commercially attractive solution. Only in the past decade publicly available cloud services emerged, which made these technologies, on the one hand, available to the developer, and on the other hand, understandable for the business community. But many of the features that make cloud computing attractive can conflict with traditional information security models. Based on a common vulnerability assessment system, which allows to determine the qualitative index of susceptibility to vulnerabilities of information systems taking into account environmental factors, a methodology for risk assessment for different types of deployment of cloud environments was proposed. Based on the widely used Common Vulnerability Accounting System, which helps to determine the qualitative indicator of susceptibility to information system vulnerabilities, the article proposes a classification of vulnerabilities typical for different types of cloud deployment.

Keywords: information security, cloud computing, vulnerability, risk model, risk assessment.

REFERENCES

1. Tsaregorodtsev, A.V. Model' otsenki riskov informatsionnoy bezopasnosti informatsionnykh sistem na osnove oblachnykh vychisleniy [Tekst] / Tsaregorodtsev, A.V., Yermoshkin, G.N. // Natsional'naya bezopasnost'. 2013. №6(29). P.46-54.
2. Tsaregorodtsev, A.V. Otsenka uyazvimostey dlya razlichnykh tipov razvertyvaniya oblachnykh sred [Tekst] / Tsaregorodtsev, A.V., Makarenko, Ye.V. // Bezopasnost' informatsionnykh tekhnologiy. 2014. №4. P.112-117.
3. Tsaregorodtsev, A.V. Odin iz podkhodov k otsenke riskov informatsionnoy bezopasnosti v oblachnykh sredakh [Tekst] / Tsaregorodtsev, A.V., Malyuk, A.A., Makarenko, Ye.V. // Bezopasnost' informatsionnykh tekhnologiy. – M., 2014. – №4. – P.68-74.
4. Tsaregorodtsev, A. Methodology of vulnerability assessment for various types of cloud structures [Tekst] / Tsaregorodtsev, A., Zelenina, A., Ružický, E. // Information Technology Applications. – Bratislava, Slovakia, 2017. – №1. – P.51-60.
5. Tsaregorotsev, A. Automation of the distribution process of sensitive data processing in a hybrid cloud computing environment [Tekst] / Tsaregorotsev, A., Zelenina A. // Information Technology Applications. – Bratislava, Slovakia, 2016. – №1. – P.137-149.