УДК 004.056:061.68

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

ДВУХЭТАПНАЯ ПРОЦЕДУРА КОЛИЧЕСТВЕННОЙ ОЦЕНКИ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

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

При использовании облачных сервисов организациями необходимо уделять особое внимание обеспечению безопасности своих вычислительных ресурсов и информационных активов. Это один из важных факторов при принятии решения об услугах аутсорсинга. Принятие новой модели предоставления ИТ-услуг с помощью облачных технологий и управление информационными рисками, невозможно без понимания возможных видов угроз, с которыми организации могут столкнуться. Авторами предлагается методика оценки рисков информационной безопасности, позволяющая проводить анализ защищенности облачных сервисов в условиях воздействия рассматриваемых классов угроз на ряду с комплексом эффективных мер и средств противодействия этим угрозам. Предложенная методика оценки рисков для различных типов развёртывания облачных сред направлена на выявление коэффициента противодействия возможным атакам и соотнесение величины ущерба с совокупной стоимостью владения всей инфраструктурой информационных ресурсов организации.

Ключевые слова: информационная безопасность, облачные вычисления, оценка риска, риск модель, частота применения эксплойта, урон при реализации эксплойта.

Введение

В связи с тем, что облачные вычисления несут с собой новые вызовы в области информационной безопасности (ИБ), крайне важно для организации контролировать процесс управления информационными рисками в облачной среде.

Для выбора мер по обеспечению информационной безопасности систем облачных вычислений необходим анализ возможных угроз и анализ рисков. Комплекс мероприятий должен быть осуществлен для снижения риска до приемлемого уровня.

Общая схема двухэтапного подхода по оценке рисков ИБ

Для возможности построения риск-модели облачной среды и расчета количественных показателей необходимо решить следующие научно-технические задачи [1].

1. Определить возможные риски использования облачных сред с ссылками на уязвимости и активы компании.
2. Для каждого риска сформировать перечень уязвимостей и построить базовые векторы CVSS.

3. Оценить уровень риска, предложив методику, где под риском будет пониматься комбинация частоты появления и соответствующего влияния потенциального нежелательного события, которое чаще всего связано с угрозой ИБ или нецелевого использования объекта оценки.

Показатели частоты и урона будут рассчитываться на основе показателей CVSS метрик: базовой, временной и инфраструктурной. Это потребует адаптацию текущих положений Общей системы учета уязвимостей (CVSS) для задачи расчета частоты и возможного урона.

На Рисунке 1 представлена общая схема предлагаемого двухэтапного подхода, по оценке рисков.

Первый этап: исходя из оценки урона при успешной реализации эксплойта, определить состояния модели.

Второй этап: исходя из оценки частоты применения эксплойта, определить состояния модели.

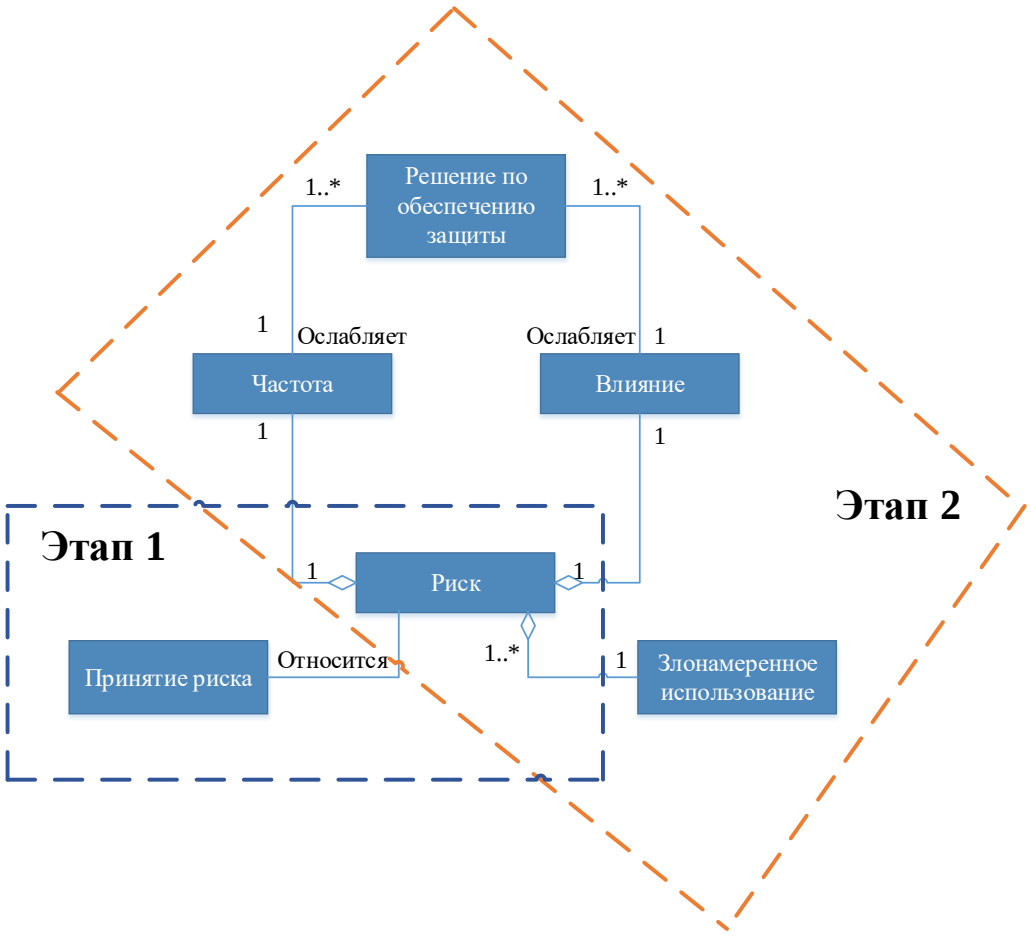

Рисунок 1 – Верхнеуровневое описание двухэтапного подхода по оценке риска

Этап 1 показывает управляемый риском анализ, который оценивает набор злонамеренных использований и связанных с ними уровней риска, и

сравнивает полученные значения с критериями принятия риска. В результате этой фазы фиксируются риски для последующих обработок. Набор этих рисков, 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.

На Рисунке 2 представлены ключевые сущности и их взаимосвязи первого этапа предлагаемого подхода, по оценке риска. Все эти составляющие необходимы для определения уровня риска и его оценки с целью понимания, какому риску требуется обработка.

При этом расчет риска осуществляется посредством сопоставления его частоты с одним из влияний для каждого злонамеренного использования. Это значит, что злонамеренное использование приведет к появлению одного или нескольких рисков ИБ, зависящих от количества связанных влияний. Эти два показателя – влияние и частота, можно определить на основании данных с помощью количественного метода оценки из общедоступных источников, к примеру – БД уязвимости NVS и CVSS.

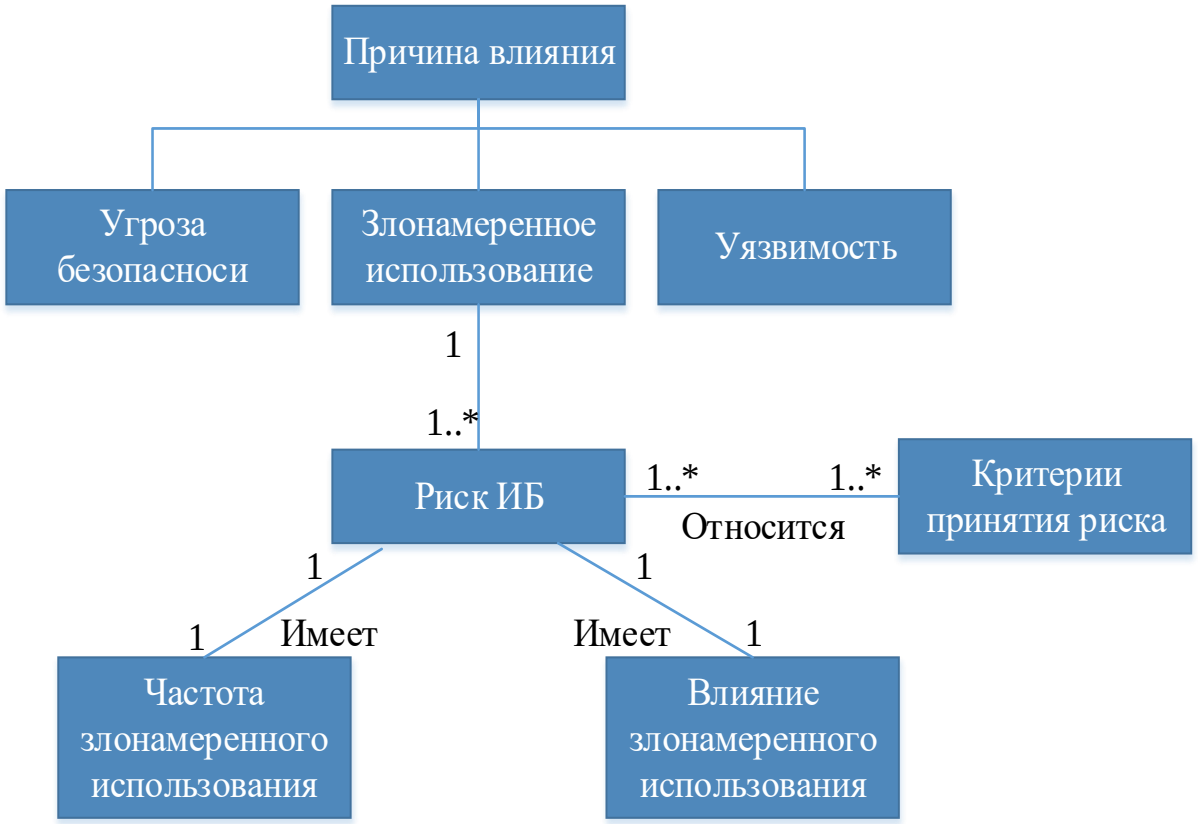

Рисунок 2 – Этап 1. Показатели расчета уровня риска

Частота злонамеренного использования и его влияние могут быть представлены в виде количественных показателей: определенное

количество проявлений в течение временного интервала или вероятность появления злонамеренного использования в определенный период времени [2]. Представить влияние можно в виде потери репутации, финансовых потерь, и др.

Представим потери для риск-модели, отраженной на Рисунке 3:

$$\{(I_1, F_1), (I_2, F_2), \dots, (I_n, F_n)\} \quad (1)$$

где F_i – это интенсивность потока событий или вероятность появления злонамеренного события, которое может привести к возникновению влияния I_i.

Множество потерь $\{L_1, L_2, L_i\}$ представим в виде:

$$\text{Статистические ожидаемые потери} = (I_1 \times F_1) \times L_1 + (I_i \times F_i) \times L_i + \dots + (I_n \times F_n) \times L_n \} \quad (2)$$

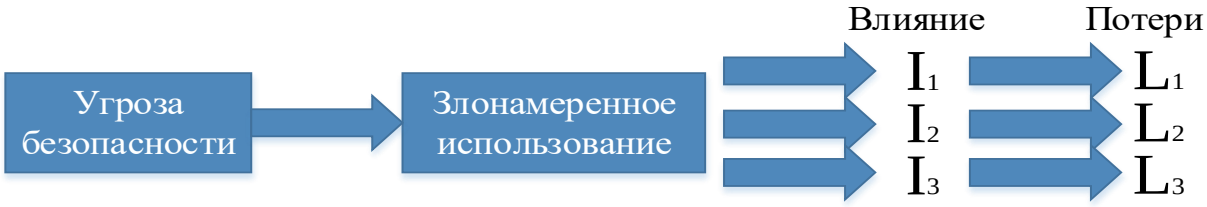

Рисунок 3 – Пример риск модели

Используя полученные выражения можно интерпретировать показатели, представить базовые положения общей системы учета уязвимостей (CVSS) относительно облачных вычислений.

Базовые положения общей системы учета уязвимостей

CVSS широко применяется и в настоящее время все чаще принимает вид стандарта для определения и оценки уязвимостей. Главная задача состоит в оценке уровня серьезности, имеющего отношение к уязвимостям и предоставление рекомендаций по снижению результатов угроз. Базовый, временной и инфраструктурный векторы приведены в Таблице 1.

Таблица 1 – Показатели требований к безопасности

Группа метрик	Вектор
Базовая	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Временная	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
Инфраструктурная	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/IR:[L,M,H,ND]/AR:[L,M,H,ND]

Общую систему учета уязвимостей можно использовать для классификации уязвимостей облачных сред (Рисунок 4).

Рисунок 4 – Группа метрик

Используем основные положения CVSS для определения частоты и влияния. Для этого скомбинируем особым образом показатели метрик.

Чем больше уровень подверженности уязвимости применению эксплойта, тем выше шанс злоумышленника для проведения успешной атаки и выше показатель частоты злонамеренного использования (F).

Рассчитаем этот показатель для каждой уязвимости, представленной в риск-модели с предположением, о том, что главные характеристики уязвимости будут описаны базовой метрикой, а учет показателей временной метрики позволит снизить вероятность успешного применения эксплойта. Таблицы 2 и 3 описывают выбранные для анализа показатели с соответствующими весами CVSS.

Таблица 2 – Показатели CVSS для расчета частоты злонамеренного использования

Группа метрик	Показатель	Значение показателя	Вес
Базовая	Вектор доступа (AV)	Локальный доступ (L)	0,395
		Сопряженная сеть (A)	0,646
		Сеть (N)	1
	Вектор сложности (AC)	Высокий (H)	0,35
		Средний (M)	0,61
		Низкая (L)	0,71
	Аутентификация (Au)	Многоразовая	0,45
		Одноразовая	0,56
		Отсутствует	0,704
Временная	Показатели доступности кода и техники эксплойта (Au)	Теория (нет доказательств) (U)	0,85
		Эксперимент (POC)	0,9
		Функциональная (F)	0,95
		Высокая (H)	1
	Показатели степени готовности решения (RL)	Официальный патч (OF)	0,87
		Временное решение (TF)	0,9
		Решение на основе рекомендаций (W)	0,95
		Отсутствует (U)	1
	Показатели степени достоверности информации (RC)	Носит предположительный характер (UC)	0,9
		Не проработано (UR)	0,95
		Подтверждено(C)	1

Таблица 3 – Показатели CVSS для расчета влияния (урона) злонамеренного использования

Группа метрик	Показатель	Значение показателя	Вес
Базовая	Воздействие на конфиденциальность (C)	Отсутствует (N)	0
		Частичное (P)	0,275
		Полное (C)	0,66
	Воздействие на целостность (I)	Отсутствует (N)	0
		Частичное (P)	0,275
		Полное (C)	0,66
	Воздействие на доступность (A)	Отсутствует (N)	0
		Частичное (P)	0,275
		Полное (C)	0,66
Инфраструктурная	Требования к конфиденциальности (CR)	Низкие (L)	0,5
		Средние (M)	1,0
		Высокие (H)	1,51
	Требования к целостности (IR)	Низкие (L)	0,5
		Средние (M)	1,0
		Высокие (H)	1,51
	Требования к доступности (AR)	Низкие (L)	0,5
		Средние (M)	1,0
		Высокие (H)	1,51
	Сопутствующий потенциальный ущерб (CDP)	Низкий (L)	0,1
		Низкий - средний (LM)	0,3
		Средний – высокий (MH)	0,4
		Высокий (H)	0,5

Использование 3 показателей базовой и 3 показателей временной метрик позволят определить частоту злонамеренного использования. Базовая метрика описывает характеристики уязвимости и её подверженность к применению эксплойта, поэтому её показатели выбраны для определения оценки начальной частоты:

$$F_{нач} = \int P(AV, AC, Au). \quad (3)$$

Начальная частота злоупотреблений может обновляться во времени. Обновление происходит в два шага: рассчитывается фактор обновления (4), затем этот фактор применяется к начальной частоте для оценки итоговой частоты применения эксплойта.

$$F_{ФО} = \int P(E, RL, RC), \quad (4)$$

$$F = \int (F_{нач} \times F_{ФО}). \quad (5)$$

Затем полученную оценку необходимо пронормировать в интервале [0;1], что позволит интерпретировать полученные значения, как показано в Таблице 4.

Таблица 4 – Значения частоты применения эксплойта

Значение	Возможность использования эксплойта
0	Уязвимость недоступна
[0;0,5]	Малая
[0,5;1]	Высокая
1	Уязвимость будет реализована

Введем новый показатель I, который будет описывать урон организации при успешной реализации эксплойта. Для этого используются три атрибута базовой (C, I, A) и 4 атрибута инфраструктурной метрик (CR, IR, AR, CDP).

Аналогично показателю частоты применения эксплойта, базовая метрика используется для определения начального урона, который представляет собой вектор конфиденциальности, целостности и доступности:

$$I_{нач} = [C, I, A]. \quad (6)$$

Инфраструктурные метрики используются для обновления начального урона с целью получения результирующей оценки. Обновление происходит в 2 этапа. На первом этапе вектор составляющих безопасности обновляется показателем сопутствующего потенциального ущерба:

$$I_{CDP} = \int CDP[C, I, A]. \quad (7)$$

После этого вектор оценок обновляется данными о требованиях безопасности, полученных из инфраструктурной метрики:

$$I_{ENV} = [CR, IR, AR]. \quad (8)$$

Результирующий вектор урона описывается выражением:

$$I = \int I_{CDP} \times I_{ENV}. \quad (9)$$

Показатель, рассчитанный по (9) отражает серьезность рассматриваемой уязвимости. Именно эта информация необходима для присвоения уязвимостей уровню сервиса при описании риск модели [3].

Заключение

Общая система оценки уязвимостей определяет качественный показатель подверженности уязвимостям с учетом факторов окружающей среды. Рассмотренная методика количественной оценки потенциальных уязвимостей для различных типов развёртывания облачных сред разработана на базе CVSS.

Предложенный подход анализа рисков позволяет проводить оценку эффективности комплекса мер и средств противодействия угрозам, а также

оценку защищенности облачных сред, функционирующих в условиях воздействия рассматриваемого класса угроз. На основе полученных оценок появляется возможность выбора наиболее подходящего варианта конфигурации облачных вычислений с точки зрения требований безопасности облачных сред.

ЛИТЕРАТУРА

1. 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.
2. 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.
3. 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.

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

TWO-STAGE PROCEDURE OF QUANTITATIVE ASSESSMENT OF INFORMATION SECURITY RISK OF CLOUD COMPUTING

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

When organizations use cloud services, special attention to ensuring the security of their computing resources and information assets should be paid. It is one of the most important factors in making decisions on outsourcing services. Adopting a new model of providing IT services using cloud technologies and managing information risks is impossible without understanding the possible types of threats that organizations may face. The authors propose a methodology for assessing information security risks that allows analyzing the cloud services security under the impact of the threat classes under consideration, as well as a set of effective measures and means to counteract these threats. The proposed method for assessing risks for different types of deployment of cloud environments is aimed at identifying the countermeasures to possible attacks and correlating the amount of damage with the total cost of ownership of the entire infrastructure of information resources of the organization.

Keywords: information security, cloud computing, risk assessment, risk model, frequency of exploit use, damage during the implementation of the exploit.

REFERENCES

1. 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.
2. 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.
3. 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.