A. A. Malyuk, A. V. Tsaregorodtsev, E. V. Makarenko

One of Approaches to Information Security Risk Estimation for Cloud Infrastructure

Keywords: cloud computing, information security threats, information risk analysis, information security requirements

Due to the fact that cloud computing bring with them new challenges in the field of information security, it is imperative for organizations to control the process of information risk management in the cloud. This paper proposes a risk assessment approach for assessing the potential damage from the attack on the implementation of components of confidential data and justify the need for the inclusion of private clouds with a high degree of protection in a hybrid cloud computing environment.

А. А. Малюк, А. В. Царегородцев, Е. В. Макаренко

ОДИН ИЗ ПОДХОДОВ К ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ СРЕДАХ

Введение

Анализ возможных угроз и анализ рисков служат основой для выбора мер по обеспечению информационной безопасности систем облачных вычислений, которые должны быть осуществлены для снижения риска до приемлемого уровня.

В то время как количественная оценка риска широко распространена в некоторых областях, таких как финансы и кредит, количественная оценка рисков информационной безопасности часто сопровождается рядом ограничений, особое место среди которых занимает отсутствие данных для проверки этих методов [1].

Предлагаемый подход к анализу и управлению рисками позволит обоснованно принимать решения при выборе систем защиты информации, программного обеспечения для компонентов информационных систем (ИС), функционирующих на основе технологии облачных вычислений.

1. Основные положения метода количественной оценки риска

Приведем определения ключевых понятий, которые будут использованы в предлагаемом подходе. *Под уязвимостью* будем понимать дефект программного обеспечения или слабость в системе безопасности, которые могут быть использованы заинтересованными лицами с целью нанесения ущерба или вреда организации. Под *известными уязвимостями* будем понимать те, которые либо не имеют патчей с исправлениями, либо имеют патчи, применяющиеся с временной задержкой. *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. Результатом использования уязвимости некоторой угрозой может стать появление нежелательного события, которое будем называть *злонамеренным использованием* [2]. Необходимо отметить, что злонамеренные использования могут возникнуть только в случае существования как угрозы, так и уязвимости и рассматриваемая уязвимость может быть использована конкретной угрозой. Это означает, что множество всех потенциальных злонамеренных событий является подмножеством набора уязвимостей и набора потенциальных угроз и, следовательно, $M =\subset ST \cap SV$, где M – набор злонамеренных событий, ST – множество угроз, SV – множество уязвимостей.

Представим метод количественной оценки рисков в виде следующих этапов (таблица 1).

Таблица 1. Метод количественной оценки риска ИБ

№	Описание этапа	
1	**Идентификация риска**	
	1.1	Идентификация угроз безопасности и влияние на активы
	1.2	Идентификация уязвимостей объекта оценки, принципов обеспечения, процессов, процедур и среды безопасности
2	**Анализ риска**	
		Оценка уровня влияния злонамеренного использования
		Оценка частоты злонамеренного использования
3	**Оценка риска**	
		Определение уровня риска для каждого набора частоты и влияния
		Оценивание риска и сравнение с критериями принятия риска
		Категоризация риска для обработки в наборы рисков
		Определение внутренних взаимосвязей между наборами рисков
		Идентификация конфликтов между наборами риска
		Назначение приоритетов наборов и рисков
		Решение найденных конфликтов
4	**Обработка риска**	
		Идентификация альтернативных решений по обеспечению безопасности и группировка их в наборы
		Идентификация эффекта и цели альтернативных систем защиты информации (СЗИ)
		Оценка и поиск оптимальной СЗИ или набора решений по обеспечению безопасности

На верхнем уровне предлагаемый подход к оценке рисков включает два основных этапа. *Первый этап* описывает управляемый риском анализ, включающий оценивание набора злонамеренных использований и связанных с ними уровней риска, которые являются результатом шагов 2, 3 предлагаемого метода, с последующим сравнением полученных значений с критериями принятия риска, которые определены на шаге 1. Результатом этой фазы является набор рисков, требующих обработки.

Набор рисков для обработки, набор альтернативных решений и других компромиссных параметров, соответствующих разработке, проекту и финансовому состоянию, являются входными данными для второго этапа метода, в рамках которого риски информационной безопасности — это проблемы и вызовы, требующие решения в виде доступных альтернативных механизмов безопасности.

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. Рис. 1 описывает ключевые сущности и их взаимосвязи первого этапа подхода по оценке риска. Все эти составляющие необходимы для определения уровня риска объекта оценки и его оценки с целью понимания, какой из рисков требует обработки.

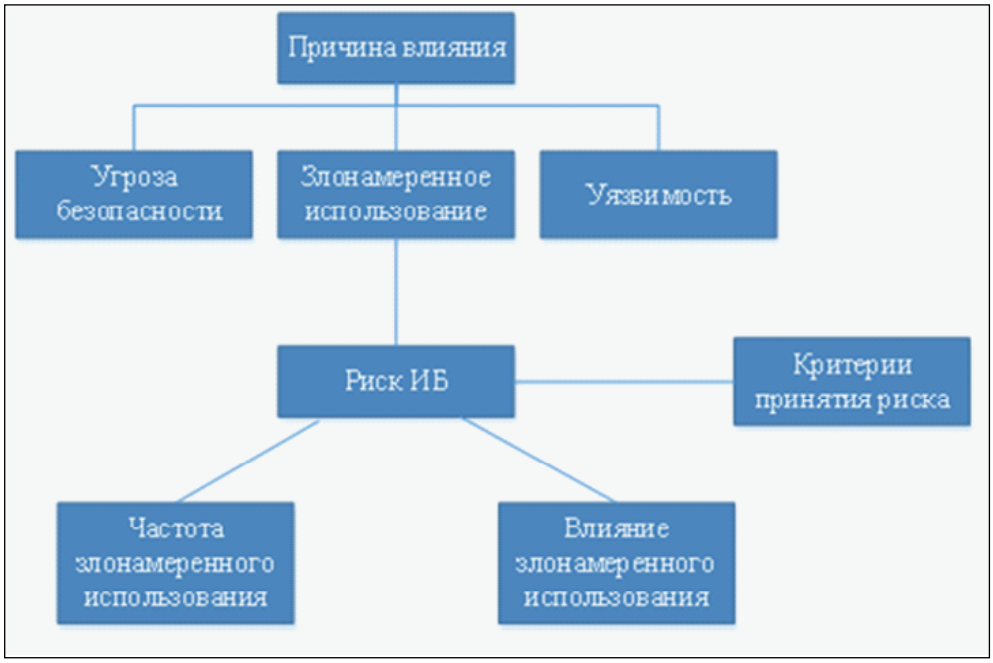

Рис. 1. Показатели для расчета уровня риска в рамках первого этапа

При этом риск рассчитывается для каждого злонамеренного использования путем комбинации его частоты с одним из влияний. Это означает, что злонамеренное использование приводит к появлению одного или нескольких рисков ИБ, зависящих от количества взаимосвязанных факторов (частота и влияние). Оба показателя (частота и влияние) могут быть определены с помощью количественного метода оценки на основании данных из общедоступных источников, одним из которых является NVD Common Vulnerability Scoring System Support (база данных уязвимостей NVS и система общего учета уязвимостей — CVSS) [3].

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. Влияние может быть представлено в виде финансовых потерь, потери репутации и т. д.

2. Определение частоты злонамеренного использования и соответствующего влияния на основе показателей CVSS

Используем основные положения методики CVSS для определения двух ключевых переменных, влияющих на оценку риска. Для этого скомбинируем особым образом показатели базовой, временной, инфраструктурной метрик. Чем выше уровень подверженности уязвимости применению эксплойта, тем больше шансов у злоумышленника провести успешную атаку и тем больше показатель *частоты злонамеренного использования* (F). Рассчитаем этот показатель для каждой уязвимости, представленной в риск-модели облачной среды, с предположением, что основные характеристики уязвимости описываются базовой метрикой, а учет показателей временной метрики позволит уменьшить вероятность успешного применения эксплойта. Тот же принцип относится и к урону (влиянию): потенциальный урон зависит от показателей уязвимости в базовой метрике, и в то же время может быть увеличен или уменьшен в зависимости от требований к конфиденциальности, доступности и целостности, определенных в инфраструктурной метрике.

Таблицы 2 и 3 описывают выбранные для анализа показатели с соответствующими весами CVSS.

Таблица 2. Показатели CVSS для расчета частоты злоупотребления

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
		Низкий (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 советов и 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

Базовая	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

Определение частоты злонамеренного использования

Использование трех показателей базовой метрики и трех показателей временной метрики позволят определить *частоту злонамеренного использования* (как часто уязвимость будет подвержена применению эксплойта). Базовая метрика описывает характеристики уязвимости и ее подверженность применению эксплойта, поэтому ее показатели выбраны для определения оценки начальной *частоты*:

$$F_{\text{нач}} = \int P(AV, AC, Au). \quad (1)$$

При этом предполагается, что начальная частота злоупотреблений может обновляться во времени. Показатели временной метрики включают в себя косвенные факторы рассматриваемой уязвимости. Обновление происходит в два шага: рассчитывается фактор обновления (ФО) (2), затем этот фактор применяется к начальной частоте для оценки итоговой частоты применения эксплойта (3).

$$F_{\text{ФО}} = \int P(E, RL, RC) \quad (2)$$

$$F = \int (F_{\text{нач}} \times F_{\text{ФО}}) \quad (3)$$

Затем полученную оценку необходимо пронормировать с целью получения значений в интервале [0;1], что позволит интерпретировать полученные значения, как показано в таблице 4.

Таблица 4. Значения частоты применения эксплойта

Значение	Интерпретация
0	Уязвимость недоступна для использования эксплойта
[0;0,5]	Возможность использования эксплойта мала

[0,5;1]	Возможность использования эксплойта высока
1	Уязвимость точно будет успешно реализована

Определение урона при успешной реализации эксплойта на основе базовой и инфраструктурной метрик

Введем новый показатель I, который будет описывать урон организации при успешной реализации эксплойта. Также этот показатель будет использован для группировки уязвимостей в определенные состояния переходной модели в виде сервисного уровня. Для этого предполагается использование трех атрибутов базовой метрики (C, I, A) и четырех атрибутов инфраструктурной метрики (CR, IR, AR, CDP), описание дано в таблице 3. Показатели инфраструктурной метрики зависят от специфики контекста использования уязвимости, включают возможный урон конфиденциальности, целостности и доступности в разрезе требований безопасности и потенциального сопутствующего ущерба конкретного состояния модели. Показатели базовой метрики описывают величину эффекта на каждую конкретную составляющую безопасности, которая впоследствии учитывается в рамках определенного контекста инфраструктурных показателей. Аналогично показателю частоты применения эксплойта, базовая метрика используется для определения начального урона, который представляет собой вектор конфиденциальности, целостности и доступности:

$$I_{\text{нач}} = [C, I, A] \,. \quad (4)$$

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

$$I_{CDP} = \int CDP[C, I, A] \,. \quad (5)$$

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

$$I_{ENV} = [CR, IR, AR] \,. \quad (6)$$

Результирующий вектор урона описывается выражением:

$$I = \int I_{CDP} \times I_{ENV} \,. \quad (7)$$

Показатель, рассчитанный по формуле 7, отражает серьезность рассматриваемой уязвимости. Именно эта информация необходима для определения требуемого уровня обслуживания, присвоения уязвимостей уровню сервиса при описании риск-модели.

Определение уровней обслуживания

Представим уровни обслуживания в виде модели переходов состояний (Марковский процесс). Первое состояние отражает отсутствие урона конфиденциальности, целостности, доступности и может быть описано в виде: [0,0; 0,0; 0,0]. Последнее состояние означает максимальный урон конфиденциальности, целостности, доступности, принимая во внимание показатели инфраструктурных метрик. Состояние [1,0; 1,0; 1,0] является поглощающим состоянием и означает отсутствие возможности применить исправление в рамках модели. Таким образом, первое состояние соответствует полному уровню сервиса *SL0*, последнее отражает отсутствие сервиса *SLx*. Все состояния между пограничными уровнями могут содержать как полный набор сервисов, так и любое количество сервисов более низкого уровня или отсутствие сервисов в зависимости от рассматриваемой модели.

3. Определение уровня риска на основе показателей частоты и урона

Для измерения уровня риска введем понятие уровня сервиса, представленного в виде Марковского процесса с непрерывным временем. Сервисные уровни зависят от проектного решения

и варианта реализации ИС, функционирующей на основе технологии облачных вычислений, структуры такой ИС и набора приложений, другими словами, от способа использования ИС.

На первом этапе определяется список уязвимостей на основании общедоступных данных, например из официальных сообщений об уязвимостях, баз данных (NVD) или путем запуска специализированных сканеров (Nessus).

Как уже было отмечено, урон от успешного применения эксплойта описывает серьезность уязвимости. Но это не означает, что две уязвимости, приводящие к одинаковому урону, имеют схожий уровень серьезности для рассматриваемой среды и приводят к соразмерному уменьшению сервисного обслуживания. В связи с этим необходимо решить задачу определения интервалов уровней серьезности уязвимостей с последующим определением для них сервисных уровней. В результате получается набор уровней сервиса от уровня без предоставления сервисов до полного набора сервисов, описанный в виде модели состояний. *Под сервисным уровнем* будем понимать непустой набор уязвимостей, имеющих уровень влияния из одного интервала.

На втором этапе исследуется модель переходов состояний, полученная на первом этапе, и дополняется интенсивностью переходов. Интенсивность переходов определяет, с какой вероятностью возможен переход из одного состояния в другое и с какой вероятностью возможно нахождение в этом состоянии в определенный интервал времени t. В модели оценки уровней риска каждое состояние ссылается на совокупный уровень серьезности набора уязвимостей. Таким образом, модель переходов состояний описывает различные уровни риска, характерные для рассматриваемой среды в момент времени t. Для определения интенсивности переходов принимается во внимание агрегированная частота использования эксплойта в определенный интервал времени.

Заключение

Предлагаемый подход к оценке рисков информационной безопасности позволяет провести оценку защищенности облачной среды, функционирующей в условиях воздействия рассматриваемого класса угроз, а также эффективности комплекса мер и средств противодействия этим угрозам. На основе полученной оценки появляется возможность сделать выбор между различными вариантами конфигурации среды облачных вычислений и выбрать наиболее приемлемый вариант с точки зрения требований безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. *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.
2. *Mell P., Grance T.* The NIST Definition of Cloud Computing, Version 15, September, 2011. [Электронный ресурс]. URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (дата обращения: 28.08.2014).
3. 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. *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.
2. *Mell P., Grance T.* The NIST Definition of Cloud Computing, Version 15, September, 2011. [Electronic resource]. URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (date of access: 28.08.14).
3. 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: 28.08.14).