УДК 004.94
doi:10.15217/issn1684-8853.2017.3.25

ПРОАКТИВНЫЙ И РЕАКТИВНЫЙ РИСК-МЕНЕДЖМЕНТ IT-СЕРВИСОВ ОБЛАЧНЫХ СРЕД

А. В. Скатков[а], *доктор техн. наук, профессор*
Д. Ю. Воронин[а], *канд. техн. наук*
В. И. Шевченко[а], *канд. техн. наук*
А. А. Ключарев[б], *канд. техн. наук, доцент*
[а]*Севастопольский государственный университет, Севастополь, РФ*
[б]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Постановка проблемы: *большинство случаев возникновения внештатных ситуаций в облачных средах является следствием неэффективного управления рисками. Например, конфликтные ситуации приводят к отказу в обслуживании и требуют принятия взвешенных, компромиссных решений по распределению ресурсов между операционными и системными процессами в облачной среде. Таким образом, задача управления рисками в облачных вычислительных средах представляется крайне актуальной.* ***Цель:*** *формализация задачи организации эффективного управления рисками в облачных вычислительных средах при использовании подходов проактивного и реактивного управления.* ***Результаты:*** *проведенный анализ основных угроз и уязвимостей облачного компьютинга выявил необходимость использования проактивного и реактивного управления рисками при формировании и реализации необходимых контрмер. Предложенный информационный портрет риска позволяет визуализировать агрегированную оценку текущего состояния облачной вычислительной среды, что является обязательным условием автоматизированного принятия оперативных решений по управлению IT-сервисами в режиме реального времени. Приведено формализованное описание жизненного цикла облачной среды при проактивном и реактивном управлении, позволяющее сформулировать проблему риск-менеджмента в классе задач динамического программирования. Сущность предлагаемого подхода состоит в последовательном, многоэтапном выборе одного из альтернативных решений, например: уменьшить вероятности возникновения неблагоприятных событий; минимизировать возможные негативные последствия при возникновении внештатных ситуаций и т. д. Новизна предлагаемого подхода состоит в том, что он может быть эффективно использован как при проактивной, так и при реактивной методике управления рисками в облачных системах.* ***Практическая значимость:*** *полученные результаты могут быть применены для визуализации оперативной обстановки в рамках комплексной системы поддержки принятия решений по управлению IT-сервисами облачных вычислительных сред. Использование предложенного информационного портрета риска позволит обеспечить требуемую реактивность и интерактивность при взаимодействии с лицом, принимающим решения.*

Ключевые слова *— облачная вычислительная среда, риск-менеджмент, информационный портрет риска, проактивное управление, реактивное управление, угроза, контрмера, динамическое программирование.*

Введение

Быстрорастущий уровень современной компьютеризации общества приводит к необходимости все более широко применять программные инструменты, в том числе технологии распределенной обработки данных. Облачные вычисления представляют собой информационную технологию для обеспечения удобного сетевого доступа к общему пулу настраиваемых вычислительных ресурсов (сетей, серверов, систем хранения данных, приложений, ресурсов, услуг и др.) по требованию, которые можно быстро активировать и предоставить с минимальными потерями на управление или минимальным взаимодействием с поставщиком услуг [1, 2]. В большинстве случаев облачные среды могут быть отнесены к объектам критического применения, для которых даже незначительные сбои при их функционировании могут приводить к существенным авариям или даже катастрофам [2–10]. Негативные последствия таких инцидентов характеризуются существенными материальными и репутационными издержками, а в некоторых случаях — даже непосредственным образом влияют на безопасность целой страны или региона.

В соответствии с работами [4–6] под риск-менеджментом понимается процесс управления рисками IT-сервисов облачных сред. В таких системах принято выделять следующие состояния [11]: безопасные, работоспособные, предкритические и аварийное. Безопасные состояния характеризуются высокой стабильностью системы, т. е. отсутствием возможности непосредственного перехода в предкритические состояния. При недостаточной эффективности процедур обеспечения гарантированной работоспособности облачная среда имеет тенденцию к деградации, т. е. переходу из работоспособных состояний в состояния, близкие к критическим. В этом случае если не будут своевременно запущены стабилизирующие процессы ее реконфигурации, то даже незначительный сбой может привести к невосстанавливаемому отказу и переходу в аварийное (поглощающее) состояние, что, например, может соответствовать отказу в вычислительном обслуживании определенного этапа

крупномасштабной научной задачи. В настоящей статье приведены результаты анализа основных угроз и уязвимостей облачного компьютинга, а также описаны ключевые особенности проактивного и реактивного подходов к риск-менеджменту.

Особенности риск-менеджмента IT-сервисов в облачных средах

В работе [10] рассматриваются различные вызовы, характерные для облачного компьютинга. Основное внимание уделено организации безопасного и конфиденциального взаимодействия облачных сервисов, которое требует наличия специалистов высокой квалификации и современного дорогостоящего оборудования. Необходимость решать проблему обеспечения конфиденциальности обрабатываемых данных является существенным ограничением при использовании облачных сервисов [13] и источником возникновения неблагоприятных событий. На примере Amazon Web Services проанализированы [13] различные подходы к идентификации угроз информационной безопасности. Очевидно, что популярность мобильных облачных сервисов требует развития подходов к обеспечению информационной безопасности, так как сложность и стоимость систем такого рода постоянно возрастает [14]. Авторы описания использования облачного аутсорсинга в Швейцарии [15] считают, что процедура миграции существенно зависит от индивидуальных характеристик компаний, таким образом, процессы риск-менеджмента должны быть адаптивными.

Существующие угрозы требуют создания эффективных технологий риск-менеджмента в облачных средах. В соответствии с работами [9, 12] принято выделять два базовых подхода к решению проблемы управления рисками — проактивный и реактивный. При проактивном управлении основной целью принимаемых решений является предупреждение возникновения различных неблагоприятных событий, приводящих к развитию рисков [9, 12]. Данный подход ориентирован на использование прогнозных оценок развития рисков и применяется для латентной части их жизненного цикла в условиях дефицита информации о величине возможных последствий развития негативных событий. Для реактивного подхода характерно наличие точных оценок последствий возникших инцидентов, и основной его целью является нейтрализация негативных последствий уже произошедших событий. Подробнее ключевые особенности проактивного и реактивного управления рисками облачных сред приведены на рис. 1.

■ ***Рис. 1.*** Ключевые особенности проактивного и реактивного управления рисками

Несмотря на существование различных подходов к оценке рисков в облачных средах [16–22], данная научная проблема остается до сих пор открытой [17]. В работе [18] предложен подход к оценке рисков информационной безопасности, который позволяет обеспечить акторов облачной вычислительной среды информацией, необходимой при принятии решений о выборе эффективного варианта взаимодействия [19]. Авторы статьи [20] предлагают использовать защитную стратегию для оценки облачных рисков. Предлагаемая экономико-основанная методология [21] реализована в программном комплексе, анализирующем корпоративные риски при использовании облачных технологий. Инструментальное средство ACRAM [22], состоящее из оффлайн- и онлайн-модулей, позволяет оценивать риск неблагоприятного размещения ресурсов потребителя при миграции в облако. Большинство современных подходов базируется на известных методах принятия решений: теории игр [23], методе анализа иерархий [24] и т. д.

К сожалению, преимущества облачной обработки данных являются причиной возникновения дополнительных угроз и уязвимостей. Можно выделить следующие особенности риск-менеджмента в облачных средах.

1. Для адекватной визуализации текущей ситуации необходимо предложить эффективные подходы, позволяющие предоставить лицу, принимающему решение (ЛПР), агрегированную оценку текущего состояния облачной вычислительной среды, что является обязательным условием автоматизированного принятия оперативных решений по управлению IT-сервисами в режиме реального времени.

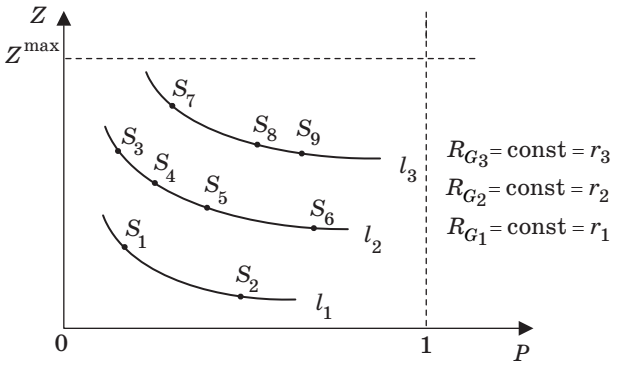
2. Процессы риск-менеджмента являются достаточно затратными, что требует внедрения адаптивных технологий запуска процедур стабилизирующей реконфигурации системы в соответствии со складывающейся информационной ситуацией.

3. Существующие подходы к формализации жизненного цикла облачной среды не в полной мере учитывают особенности проактивного риск-менеджмента.

Далее рассматриваются предлагаемые подходы к решению обозначенных проблем и системных противоречий.

Визуализация фазового пространства рисков облачной среды

Состояние облачной среды описывается точкой в n-мерном фазовом пространстве, т. е. каждая из координат описывает одну из рассматриваемых характеристик. Например, на рис. 2 изображено двухмерное пространство рисков.

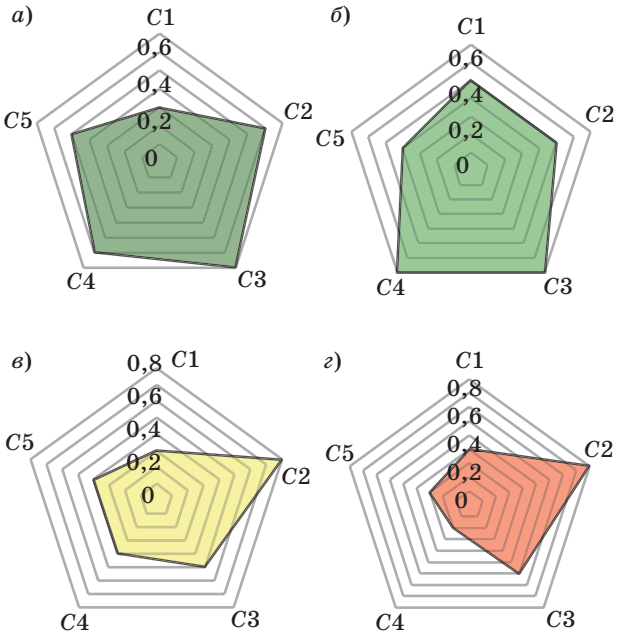


■ ***Рис. 2.*** Геометрическая интерпретация двухмерного пространства рисков облачной среды

Состояние S_i описывается кортежем $\langle P_{S_i}, Z_{S_i} \rangle$, где P_{S_i} — вероятность возникновения неблагоприятного события в состоянии S_i; Z_{S_i} — потери, обусловленные возникновением неблагоприятного события в i-м состоянии. Под альтернативными состояниями облачной среды будем понимать элементы некоторой группы, обладающие важным свойством: значения агрегированных оценок риска у них совпадают. Графически элементы такой группы изображаются на одной и той же кривой, т. е. если точка, описывающая j-е состояние системы в пространстве риска, лежит на графике l_i, то $S_j \in G_j$, $R_{G_i} = \text{const} = r_i$, $i \neq j$, где R_{G_i} — оценка риска для i-й группы эквивалентных состояний облачной среды. Будем считать, что $\forall i \in (0, |S|)$: $Z_{S_i} \in \left[0, Z^{\max}\right]$, $P_{S_i} \in [0,1]$. Двухмерное пространство рисков удобно использовать ЛПР при поиске компромиссных решений, для которых можно обеспечить улучшение одного из параметров риска (P или Z) за счет ухудшения другого без последующего увеличения агрегированной оценки риска. Это позволяет сделать процесс управления рисками более гибким и существенно расширяет область допустимых решений [11]. Однако двухмерное пространство риска, учитывающее зависимость только между компонентами риска P и Z, при решении ряда задач не всегда достаточно.

Для детальной визуализации характеристик состояний IT-сервисов облачной среды по аналогии с понятием информационного портрета [25] необходимо построить информационный портрет облачного риска. Здесь и далее под информационным портретом риска будем понимать выпуклую оболочку множества — некоторый профиль точек, описывающий риск состояний облачной среды. Например, на рис. 3, *а–г* изображены информационные портреты облачного риска для состояний S_1, S_2, S_3, S_7.

При визуализации анализировались значения нормированных характеристик эффективности



■ ***Рис. 3.*** Информационный портрет риска для состояния S_1 (*а*); S_2 (*б*); S_3 (*в*); S_7 (*г*)

функционирования облачной среды, описанные кортежем $CC = <C_1, C_2, C_3, C_4, C_5>$, где C_i — элемент кортежа, сопоставленный обобщенной оценке риска для *i*-й группы рисков, например, информационных, ресурсных, операционных, финансовых, социальных. Следует отметить, что цвет заливки внутренней области информационного портрета облачного риска может варьироваться. Он зависит от агрегированной оценки риска R_{G_i}, вычисленной для анализируемого состояния облачной вычислительной среды.

Эта обобщенная оценка осуществляется на основе информационных признаков кортежа *CC* и системы правил вида if-then-otherwise:

$$\begin{cases} \text{if}\left[\left(C_1(S_i) > C_1^{\text{гр}}\right) \cup \left(C_2(S_i) > C_2^{\text{гр}}\right) \cup \ldots \right. \\ \left. \cup \left(C_k(S_i) > C_k^{\text{гр}}\right)\right], \text{ then}\left[S_i \in S^{\text{б}}\right]; \\ \ldots \\ \text{if}\left[\left(C_1(S_i) > C_1^{\text{гр}}\right) \cup \left(C_2(S_i) < C_2^{\text{гр}}\right) \cup \ldots \right. \\ \left. \cup \left(C_k(S_i) = C_k^{\text{гр}}\right)\right], \text{ then}\left[S_i \in S^{\text{р}}\right]; \\ \ldots \\ \text{if}\left[\left(C_1(S_i) \le C_1^{\text{гр}}\right) \cup \left(C_2(S_i) \le C_2^{\text{гр}}\right) \cup \ldots \right. \\ \left. \cup \left(C_k(S_i) \le C_k^{\text{гр}}\right)\right], \text{ then}\left[S_i \in S^{\text{прк}}\right]; \\ \ldots \\ \text{otherwize}\left[S_i \in S^{\text{п}}\right], \end{cases}$$

где $S^{\text{б}}$ — подмножество безопасных состояний облачной среды; $S^{\text{р}}$ — подмножество работоспособных состояний облачной среды; $S^{\text{прк}}$ — подмножество предкритических состояний облачной среды; $S^{\text{п}}$ — аварийное, поглощающее состояние; $C_j^{\text{гр}}$ — скалярная величина, задающая пороговое значение критичности для *j*-го элемента кортежа *CC*. Для различных предметных областей $C_j^{\text{гр}}$ различна и определяется как при учете особенностей функционирования конкретной облачной среды, так и в соответствии со складывающейся ситуацией.

Для состояний облачной среды предлагается различать три уровня риска (соответствуют различным цветам заливки информационного портрета):

1) уровень уверенного функционирования облачной среды (зеленый цвет) — анализируемое состояние является безопасным и описывается элементом подмножества $S^{\text{б}}$;

2) уровень существенного риска (желтый цвет) — среда находится в работоспособном состоянии, однако вероятность перехода системы в предкритическое состояние слишком высока;

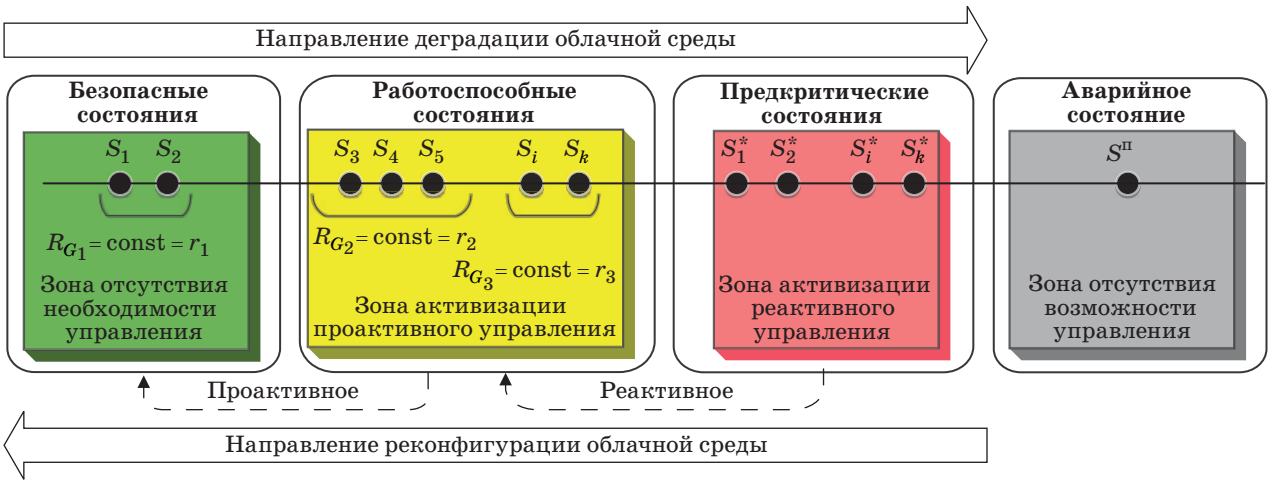
3) уровень неприемлемого риска (красный цвет) — анализируемое состояние облачной среды относится к подмножеству предкритических состояний $S^{\text{прк}}$, и любой незначительный сбой в системе может привести к переходу в аварийное, невозвратное состояние.

Таким образом, предложенный информационный портрет риска является удобным средством визуализации системных характеристик, описывающих состояния облачной среды, и может быть использован ЛПР при принятии оперативных решений по управлению IT-сервисами.

Жизненный цикл облачной среды при проактивном и реактивном управлении

Проактивный подход ориентирован в основном на использование превентивных мер и эффективен как для весьма сложных, так и для относительно динамичных систем. С другой стороны, управляющие воздействия при реактивном подходе более затратные, чем при проактивном, но и реализуются сравнительно реже. Реактивный подход позволяет сэкономить на мониторинге, но при этом вероятность попасть в аварийное состояние становится существенно выше. Известно [2–9], что целью реактивного управления является недопущение переходов объекта критического применения в состояния, имеющие «неприемлемый» уровень риска, а проактивного — в состояния, имеющие «существенный» уровень риска.

Обобщенная диаграмма (рис. 4) позволяет систематизировать динамику состояний жизненного цикла облачной среды.



■ ***Рис. 4.*** Обобщенная диаграмма динамики состояний жизненного цикла облачной среды

Состояния облачной среды изображены точками и описываются при помощи множества $S = S^{\text{б}} \cup S^{\text{р}} \cup S^{\text{прк}} \cup S^{\text{п}}$; $S^{\text{б}} \cap S^{\text{р}} \cap S^{\text{прк}} \cap \cap S^{\text{п}} = \varnothing$, подмножества $S^{\text{б}} = \left\{ S_1, S_2, \ldots, S_{|S^{\text{б}}|} \right\}$, $S^{\text{р}} = \left\{ S_i, \ldots, S_k, \ldots, S_{|S^{\text{р}}|} \right\}$, $S^{\text{прк}} = \left\{ S_i^*, \ldots, S_k^*, \ldots, S_{|S^{\text{прк}}|} \right\}$. С точки зрения функционирования облачной среды переходы между ее состояниями могут быть как конструктивные, так и деструктивные (согласно схеме, представленной на рис. 4). Под влиянием деградационных процессов происходят переходы между состояниями слева направо, а при успешных процедурах реконфигурации — справа налево.

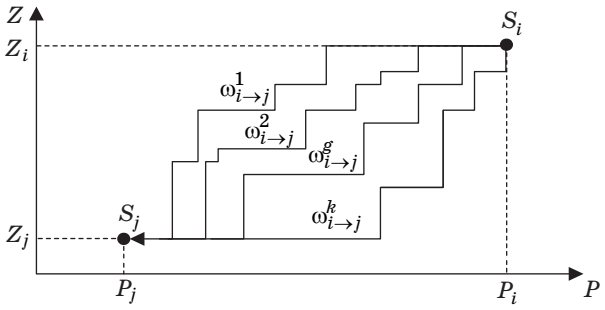
Цель проактивного управления: необходимо $\forall t = \{1, 2, \ldots, w\}$ найти такое управление $u^{\text{опт}}(t) = \arg \max_{u_i(t) \in U^{\text{д}}(t)} \Phi\left(u_i(t), t\right)$ при выполнении ограничения $S(u_i(t), t) \in S^{\text{б}}$, где w — число моментов времени при синхронном управлении облачной средой; $U^{\text{д}}(t)$ — множество допустимых управлений в момент времени t; $\Phi(u_i(t), t)$ — функция, оценивающая эффективность управления $u_i(t)$ в момент времени t.

Цель реактивного управления: $\forall t = \{1, 2, \ldots, w\}$ необходимо найти управление $u^{\text{опт}}(t) = \arg \max_{u_i(t) \in U^{\text{д}}(t)} \Phi\left(u_i(t), t\right)$ при одновременном выполнении ограничений $S(u_i(t), t) \notin S^{\text{прк}}$ и $S(u_i(t), t) \notin S^{\text{п}}$.

Несмотря на описанные различия, присутствующие в концепциях реактивного и проактивного подходов, для них можно сформулировать общую стратегическую директиву: реконфигурация облачной среды сводится к поиску такой последовательности управлений, которая обеспечила бы наиболее эффективную траекторию перемещения из текущего состояния в желаемое при строгом соблюдении заданных выше ограничений. Под траекторией будем понимать последовательность состояний облачной среды при движении из состояния S_i в состояние S_j. Постановки данной задачи могут варьироваться в зависимости от доступности априорной информации, подхода к управлению (проактивный или реактивный) и выбранного метода решения. Например, координаты состояний в фазовом пространстве рисков могут быть заданы детерминированно либо стохастически; для каждого управления априорно могут быть известны полные или приближенные оценки его эффективности в рассматриваемый момент времени и т. д. Все это требует создания единого универсального инструментального средства, позволяющего принимать решения как в автоматическом, так и в автоматизированном режиме, эффективно используя неформализованный опыт ЛПР.

Рассмотрим постановку базового варианта задачи риск-менеджмента для случая двухмерного пространства рисков (траектории управления риском облачной среды проиллюстрированы на рис. 5).

Предполагается, что за один переход между состояниями возможно реализовать только одно из управлений: уменьшить вероятность возникновения неблагоприятного события либо уменьшить потери, связанные с его появлением. То есть между любыми двумя состояниями некоторой траектории управляющее воздействие формирует величину уменьшения одной из альтернативных характеристик — P либо Z. Последовательность управлений $U_{i \to j}^m = \left\{ u_1^m, u_2^m, \ldots, u_{|U^m|}^m \right\}$ формирует m-ю траекторию $\omega_{i \to j}^m = \left\{ S_i, \ldots, S_k, \ldots, S_j \right\}$.



■ ***Рис. 5.*** Траектории управлений риском облачной среды

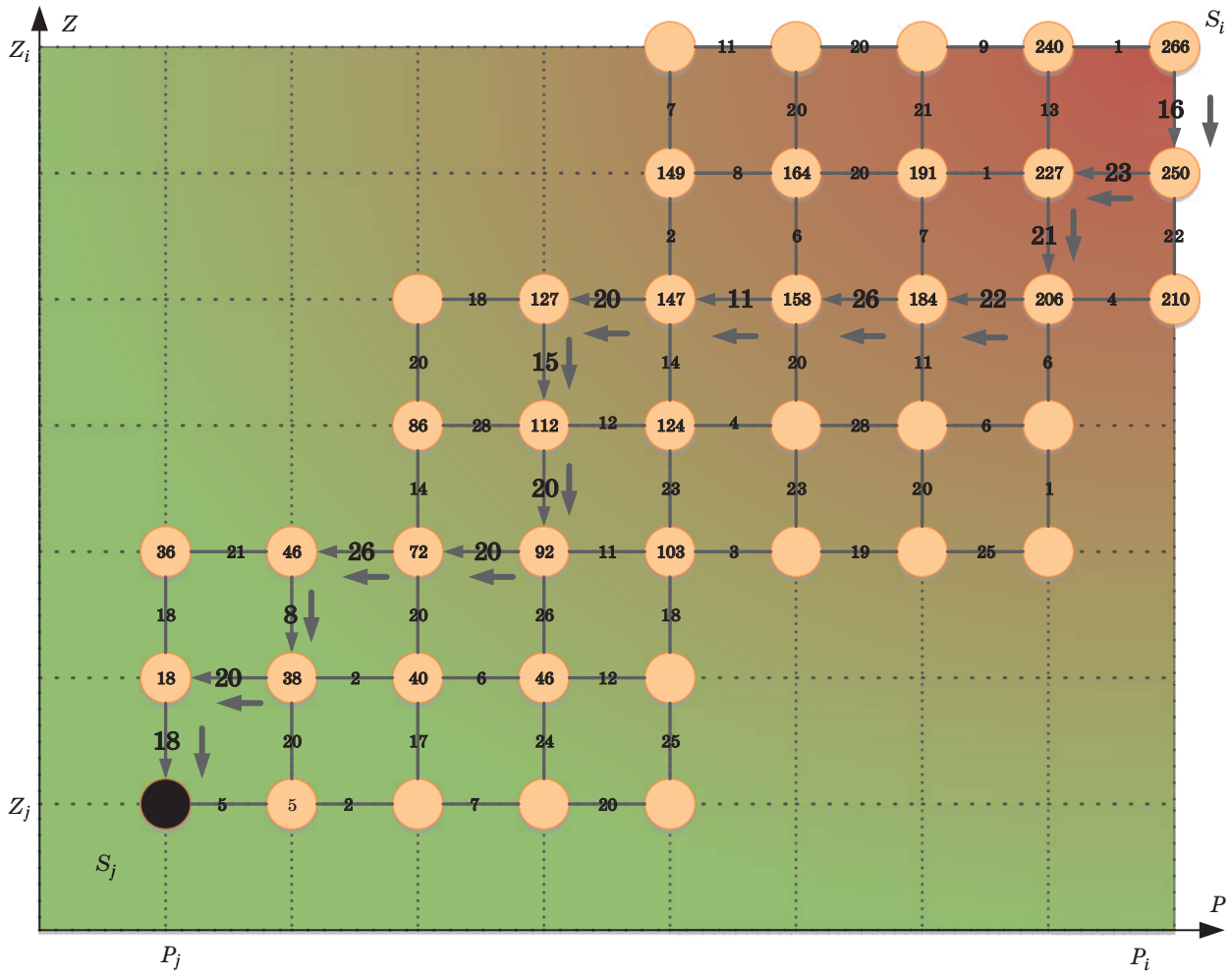
Формализация постановки задачи состоит в следующем.

Дано: $\left\langle S_i, S_j, \left\langle P_{S_i}, Z_{S_i}\right\rangle, \left\langle P_{S_j}, Z_{S_j}\right\rangle, \Omega_{\text{д}}^{i\to j}, \Theta\right\rangle$, где $\Omega_{\text{д}}^{i\to j} = \left\{U^1, U^2, \ldots, U^g, \ldots, U^k, \ldots, U^{\left|\Omega_{\text{д}}^{i\to j}\right|}\right\}$ — множество допустимых последовательностей управлений при переходе из S_i в S_j; $\Theta(U^m)$ — функция, оценивающая эффективность последовательности управлений при реализации траектории.

Найти: $U_{i\to j}^{\text{опт}} = \arg \max\limits_{U^m \in \Omega_{\text{д}}^{i\to j}} \Theta\left(U^m\right)$.

Применение подходов динамического программирования при решении задачи облачного риск-менеджмента

Для поиска эффективного управления риском облачной среды предлагается применить методы динамического программирования [26]. Введем упрощающее допущение: за один шаг управления может быть уменьшено альтернативно только P либо Z. Исходные данные $\left\langle S_i, S_j, \left\langle P_{S_i}, Z_{S_i}\right\rangle, \left\langle P_{S_j}, Z_{S_j}\right\rangle, \Omega_{\text{д}}^{i\to j}, \Theta\right\rangle$ представлены на рис. 6. Координаты точки S_i равны $\left\langle P_{S_i}, Z_{S_i}\right\rangle$, для S_j — $\left\langle P_{S_j}, Z_{S_j}\right\rangle$. Для каждого допу-



■ ***Рис. 6.*** Пример решения задачи управления рисками облачной среды при использовании динамического программирования

стимого управления (представлены дугами) известны оценки эффективности (отображены возле дуг).

В узлах представлены наилучшие оценки эффективности достижения соответствующего состояния облачной среды. Интервалы $[P_{S_j}, P_{S_i}]$ и $[Z_{S_j}, Z_{S_i}]$ имеют одинаковую длину, что дает возможность пользоваться методами динамического программирования. Каждый такой интервал представляет собой определенный этап решения задачи, его результат — выбор эффективного управления для движения между соседними состояниями. Множество допустимых траекторий перехода из *i*-го состояния в *j*-е формируется перечислениями различных путей между узлами, описывающими состояния *i* и *j*. Для каждой траектории множество дуг, которое ее составляет, задано априорно. Для того чтобы оценить эффективность траектории, надо просуммировать эффективности управлений, которые описываются весами соответствующих дуг. Безусловно, представленную задачу можно было бы решить и полным перебором всех возможных траекторий, однако метод динамического программирования выдаст результат той же точности, но трудоемкость вычислений при этом будет существенно снижена. Результат решения задачи представлен на рис. 6. Оптимальная траектория движения из *i*-го состояния в *j*-е выделена стрелками. Ее эффективность равна 266 усл. ед.

Полученная базовая формализация задачи управления рисками облачных сред может быть дополнена ограничениями, характерными только для проактивного либо для реактивного подхода к управлению рисками. На выбор метода ее решения существенное влияние может оказать уровень доступной априорной информации о кортеже $\left\langle S_i, S_j, \left\langle P_{S_i}, Z_{S_i} \right\rangle, \left\langle P_{S_j}, Z_{S_j} \right\rangle, \Omega_{\text{д}}^{i \to j}, \Phi, \Theta \right\rangle$. Необходимость парирования дефицита этой информации существенно усложнит рассматриваемую задачу и потребует синтеза соответствующих информационных технологий, методов и инженерных решений, ориентированных на оказание квалифицированной интерактивной поддержки ЛПР при принятии решений в данной предметной области.

Заключение

Организация риск-менеджмента в облачных средах является нетривиальной, противоречивой научно-практической задачей. Обилие различных подходов к анализу угроз, оценке рисков и формированию необходимых контрмер существенно усложняет и без того трудоемкую задачу поиска компромисса при распределении ресурсов между сервисными и операционными процессами в критических вычислительных системах. Предложенная формализация данной задачи, в отличие от существующих подходов, предоставляет возможность интеграции различных проактивных и реактивных методик риск-менеджмента облачных систем, что позволяет Брокеру, с одной стороны, прогнозировать наступление рисковых событий, а с другой — принимать оперативные решения по минимизации потерь, связанных с возникновением неблагоприятных событий. В частности, предложенный информационный портрет позволяет визуализировать агрегированную оценку риска для текущего состояния облачной вычислительной среды, что является обязательным условием принятия эффективных решений в режиме реального времени. Приведенный числовой пример иллюстрирует возможность использования методов динамического программирования при решении задач риск-менеджмента для случаев, когда размерность фазового пространства состояний системы является сравнительно малой.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, грант № 15-29-07936.

Литература

1. **Erl T., Puttini R., Mahmood Z.** Cloud Computing: Concepts, Technology & Architecture. — Pearson Education, 2013. http://servicetechbooks.com/pdf/cloud_sample_chapter_1.pdf (дата обращения: 15.10.2016).
2. **Nelson L. S., Raouf B.** Cloud Architectures, Networks, Services, and Management. — John Wiley & Sons, 2015. http:// onlinelibrary. wiley. com/ book/ 10.1002/ 9781119042655 (дата обращения: 15.10.2016).
3. **Catteddu D., Hogben G.** Cloud Computing: Benefits, Risks and Recommendations for Information Security. — ENISA, 2009. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment (дата обращения: 15.10.2016).
4. **Damenu T. K., Balakrishna C.** Cloud Security Risk Management: A Critical Review // Proc. of the 9th IEEE Intern. Conf. on Next Generation Mobile Applications, Services and Technologies. 2015. P. 370–375. doi:10.1109/NGMAST.2015.25
5. **Ku F. C., Chen T. C.** The Risk Management Strategy of Applying Cloud Computing // Intern. Journal of Advanced Computer Science and Applications (IJACSA). 2012. N 9. P. 18–27.
6. **Fitó J. O., Macías M. L., Fernández J. G.** Toward Business-driven Risk Management for Cloud Computing // Proc. of the Intern. Conf. on Network and Service

Management. 2010. P. 238–241. doi:10.1109/CNSM.2010.5691291
7. **Habib S. M., Ries S., Muhlhauser M.** Towards a Trust Management System for Cloud Computing // Proc. of the 10th Intern. Conf. on Trust, Security and Privacy in Computing and Communications. 2011. P. 933–939. doi:10.1109/TrustCom.2011.129
8. **Grobauer B., Walloschek T., Stocker E.** Understanding Cloud Computing Vulnerabilities // Security & Privacy. 2011. N 2. P. 50–57. doi:10.1109/MSP.2010.115
9. **Охтилев М. Ю., Мустафин Н. Г., Миллер В. Е., Соколов Б. В.** Концепция проактивного управления сложными объектами: теоретические и технологические основы // Изв. вузов. Приборостроение. 2014. Т. 57. № 11. С. 7–14.
10. **Takabi H., Joshi J. B., Ahn G. J.** Security and Privacy Challenges in Cloud Computing Environments // Security & Privacy. 2010. N 6. P. 24–31. doi:10.1109/MSP.2010.186
11. **Скатков А. В.** и др. Информационные технологии для критических инфраструктур: монография. — Севастополь: Изд-во СевНТУ, 2012. — 306 с.
12. **Саввин А.** Круги без границ. Человек, бизнес и информационные технологии как единая система. — М.: Юнайтед Пресс, 2010. — 160 с.
13. **Mosca P., Zhang Y., Xiao Z., and Wang Y.** Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services // Intern. Journal of Communications, Network and System Sciences. 2014. N 12. P. 529–535. doi:10.4236/ijcns.2014.712053
14. **Sang-Ho Na, Kyung-Hun Kim, and Eui-Nam Huh.** Threats Evaluation for SLAs in Cloud Computing // Proc. of the IEEE Intern. Conf. on Convergence Technology. 2013. P. 1570–1571.
15. **Brender N., Markov I.** Risk Perception and Risk Management in Cloud Computing: Results from a Case Study of Swiss Companies // Intern. Journal of Information Management. 2013. N 5. P. 726–733. doi:10.1016/j.ijinfomgt.2013.05.004
16. **Saripalli P., Walters B.** QUIRC: A Quantitative Impact and Risk Assessment Framework // Proc. of the IEEE 3rd Intern. Conf. on Cloud Computing. 2010. P. 280–288. doi:10.1109/CLOUD.2010.22
17. **Theoharidou M., Tsalis N., Gritzalis D.** In Cloud we Trust: Risk-Assessment-as-a-Service // Proc. of the Intern. Conf. on Trust Management. 2013. P. 100–110.
18. **Sangroya A., Kumar S., Dhok J., and Varma V.** Towards Analyzing Data Security Risks in Cloud Computing Environments // Proc. of the Intern. Conf. on Information Systems, Technology and Management. 2010. P. 255–265. doi:10.1007/978-3-642-12035-0_25
19. **Skatkov A. V., Maschenko E. N., Shevchenko V. I., Voronin D. Y.** Actors Interactions Research in Cloud Computing Environments Using System Dynamics Methodology // Proc. of the 18th FRUCT & ISPIT Conf. 2016. P. 612–619.
20. **Zhu S. C., Xu Y., Jin M. Y., Sheng L.** Cloud Computing Security Risk Assessment Based on Level Protection Strategy // Computer Security. 2013. N 5. P. 39–42.
21. **Bellandi V.,** et al. Toward Economic-Aware Risk Assessment on the Cloud // Security & Privacy. 2015. N 6. P. 30–37. doi:10.1109/MSP.2015.138
22. **Chih C. A., Huang Y. L.** An Adjustable Risk Assessment Method for a Cloud System // Proc. of the IEEE Intern. Conf. on Software Quality, Reliability and Security. 2015. P. 115–120. doi:10.1109/QRS-C.2015.27
23. **Skatkov A. V., Shevchenko V. I., and Voronin D. Y.** Game-theoretical Management Model for IT-services of ERP-systems Guaranteed Level Assurance in Cloud Environments // Proc. of the 5th IEEE Intern. Conf. on Informatics, Electronics & Vision, Dhaka, Bangladesh. 2016. P. 1113–1116. doi:10.1109/ICIEV.2016.7760172
24. **Jiang Z. W., Zhao W. R., Liu Y., Liu B. X.** Model for Cloud Computing Security Assessment Based on Classified Protection // Computer Science. 2013. N 8. P. 151–156.
25. **Карабутов Н. Н.** Структурная идентификация систем: анализ динамических структур. — М.: МГИУ, 2008. — 160 с.
26. **Bellman R. E.** Dynamic Programming. — Princeton University Press, 2010. — 392 p.

UDC 004.94
doi:10.15217/issn1684-8853.2017.3.25

Proactive and Reactive Risk Management of IT Services of Cloud Environments

Skatkov A. V.[a], Dr. Sc., Tech., Professor, AVSkatkov@sevsu.ru
Voronin D. Y.[a], PhD, Tech., Associate Professor, dima@voronins.com
Shevchenko V. I.[a], PhD, Tech., Associate Professor, kvt.sevntu@gmail.com
Klyucharev A. A.[b], PhD, Tech., Associate Professor, ak@aanet.ru
[a]Sevastopol State University, 33, Universitetskaya St., 299053, Sevastopol, Russian Federation
[b]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: Most of emergencies in cloud environments are the results of ineffective risk management. For example, conflict situations lead to a service denial and require balanced and compromise solutions on resource allocation between the operating and systemic processes in the environment. Thus, the problem of risk management in cloud computing environments is extremely urgent. **Purpose:** We need to formalize the problem of effective risk management in cloud environments using the approaches with proactive

or reactive control. **Results:** The conducted analysis of the main threats and vulnerabilities of cloud computing has identified the need of proactive or reactive risk management in order to form and implement the necessary countermeasures. The proposed information portrait of a risk allows you to visualize the aggregated assessment of the current state of a cloud computing environment, which is an indispensable condition for automated operational decision-making in real-time IT service management. A formalization has been given for a life cycle of a cloud environment supporting proactive or reactive control. This allows you to formulate the risk management problem in terms of dynamic programming. The essence of the proposed method is sequential multistage choice of one of alternative solutions, such as reducing the probability of adverse events, minimizing possible negative consequences of emergency situations, etc. The novelty of the proposed approach implies that it can be effectively used for either proactive or reactive risk management in cloud systems. **Practical relevance:** The obtained results can be used to visualize the operative situation within an integrated decision-support system aimed to manage IT services of cloud computing environments. The usage of the proposed information portrait of a risk will provide the necessary reactivity and interactivity of the interaction with the decision maker.

Keywords — Cloud Computing Environment, Risk Management, Information Portrait of a Risk, Proactive Management, Reactive Management, Threat, Countermeasure, Dynamic Programming.

References

1. Erl T., Puttini R., Mahmood Z. *Cloud Computing: Concepts, Technology & Architecture*. Pearson Education, 2013. Available at: http://servicetechbooks.com/pdf/cloud_sample_chapter_1.pdf. (accessed 15 October 2016).
2. Nelson L. S., Raouf B. *Cloud Architectures, Networks, Services, and Management*. John Wiley & Sons, 2015. Available at: http://onlinelibrary.wiley.com/book/10.1002/9781119042655. (accessed 15 October 2016).
3. Catteddu D., Hogben G. *Cloud Computing: Benefits, Risks and Recommendations for Information Security*. ENISA, 2009. Available at: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment (accessed 15 October 2016).
4. Damenu T. K., Balakrishna C. Cloud Security Risk Management: A Critical Review. *Proc. the 9th IEEE Intern. Conf. on Next Generation Mobile Applications, Services and Technologies*, 2015, pp. 370–375. doi:10.1109/NGMAST.2015.25
5. Ku F. C., Chen T. C. The Risk Management Strategy of Applying Cloud Computing. *Intern. Journal of Advanced Computer Science and Applications (IJACSA)*, 2012, vol. 3, no. 9, pp. 18–27.
6. Fitó J. O., Macías M. L., Fernández J. G. Toward Business-driven Risk Management for Cloud Computing. *Proc. the Intern. Conf. on Network and Service Management*, 2010, pp. 238–241. doi:10.1109/CNSM.2010.5691291
7. Habib S. M., Ries S., Muhlhauser M. Towards a Trust Management System for Cloud Computing. *Proc. 10th Intern. Conf. on Trust, Security and Privacy in Computing and Communications*, 2011, pp. 933–939. doi:10.1109/TrustCom.2011.129
8. Grobauer B., Walloschek T., Stocker E. Understanding Cloud Computing Vulnerabilities. *Security & Privacy*, 2011, vol. 9, no. 2, pp. 50–57. doi:10.1109/MSP.2010.115
9. Ohtilev M. Yu., Mustafin N. G., Miller V. E., Sokolov B. V. The Concept of Proactive Management of Complex Objects: Theoretical and Technological Bases. *Izvestija vuzov. Priborostroenie*, 2014, vol. 57, no. 11, pp. 7–14 (In Russian).
10. Takabi H., Joshi J. B., Ahn G. J. Security and Privacy Challenges in Cloud Computing Environments. *Security & Privacy*, 2010, vol. 8, no. 6, pp. 24–31. doi:10.1109/MSP.2010.186
11. Skatkov A. V., et al. *Informatsionnye tekhnologii dlia kriticheskikh infrastruktur* [Information Technology for Critical Infrastructures]. Sevastopol, SevNTU Publ., 2012. 306 p. (In Russian).
12. Savvin A. *Krugi bez granits. Chelovek, biznes i informatsionnye tekhnologii kak edinaia sistema* [Circles without Borders. Man, Business and Information Technology as a System]. Moscow, United Press Publ., 2010. 160 p. (In Russian).
13. Mosca P., Zhang Y., Xiao Z., and Wang Y. Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services. *Intern. Journal of Communications, Network and System Sciences*, 2014, vol. 7, no. 12, pp. 529–535. doi:10.4236/ijcns.2014.712053
14. Sang-Ho Na, Kyung-Hun Kim, and Eui-Nam Huh. Threats Evaluation for SLAs in Cloud Computing. *Proc. IEEE Intern. Conf. on Convergence Technology*, 2013, pp. 1570–1571.
15. Brender N., Markov I. Risk Perception and Risk Management in Cloud Computing: Results from a Case Study of Swiss Companies. *Intern. Journal of Information Management*, 2013, vol. 33, no. 5, pp. 726–733. doi:10.1016/j.ijinfomgt.2013.05.004
16. Saripalli P., Walters B. QUIRC: A Quantitative Impact and Risk Assessment Framework. *Proc. IEEE 3rd Intern. Conf. on Cloud Computing*, 2010, pp. 280–288. doi:10.1109/CLOUD.2010.22
17. Theoharidou M., Tsalis N., Gritzalis D. In Cloud we Trust: Risk-Assessment-as-a-Service. *Proc. Intern. Conf. on Trust Management*, 2013, pp. 100–110.
18. Sangroya A., Kumar S., Dhok J., and Varma V. Towards Analyzing Data Security Risks in Cloud Computing Environments. *Proc. Intern. Conf. on Information Systems, Technology and Management*, 2010, pp. 255–265. doi:10.1007/978-3-642-12035-0_25
19. Skatkov A. V., Maschenko E. N., Shevchenko V. I., Voronin D. Y. Actors Interactions Research in Cloud Computing Environments Using System Dynamics Methodology. *Proc. 18th FRUCT & ISPIT Conf.*, 2016, pp. 612–619.
20. Zhu S. C., Xu Y., Jin M. Y., Sheng L. Cloud Computing Security Risk Assessment Based on Level Protection Strategy. *Computer Security*, 2013, vol. 5, pp. 39–42.
21. Bellandi V., et al. Toward Economic-Aware Risk Assessment on the Cloud. *Security & Privacy*, 2015, vol. 13, no. 6, pp. 30–37. doi:10.1109/MSP.2015.138
22. Chih C. A., Huang Y. L. An Adjustable Risk Assessment Method for a Cloud System. *Proc. IEEE Intern. Conf. on Software Quality, Reliability and Security*, 2015, pp. 115–120. doi:10.1109/QRS-C.2015.27
23. Skatkov A. V., Shevchenko V. I., Voronin D. Y. Game-theoretical Management Model for IT-services of ERP-systems Guaranteed Level Assurance in Cloud Environments. *Proc. 5th IEEE Intern. Conf. on Informatics, Electronics & Vision, Dhaka, Bangladesh*, 2016, pp. 1113–1116. doi:10.1109/ICIEV.2016.7760172
24. Jiang Z. W., Zhao W. R., Liu Y., Liu B. X. Model for Cloud Computing Security Assessment Based on Classified Protection. *Computer Science*, 2013, vol. 8, pp. 151–156.
25. Karabutov N. N. *Strukturnaia identifikatsiia sistem: analiz dinamicheskikh struktur* [Structural Identification Systems: Analysis of Dynamic Structures]. Moscow, MGIU Publ., 2008. 160 p. (In Russian).
26. Bellman R. E. *Dynamic Programming*. Princeton University Press, 2010. 392 p.