И. Б. ПАРАЩУК, И. Б. САЕНКО
Санкт-Петербургский институт информатики
и автоматизации Российской академии наук (СПИИРАН), Санкт-Петербург

ОЦЕНКА КАЧЕСТВА ПРОЦЕССА РЕКОНФИГУРАЦИИ ПОЛИТИК РАЗГРАНИЧЕНИЯ ДОСТУПА В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Рассмотрен подход к решению задачи оценки качества процесса реконфигурации политик разграничения доступа в критически важных облачных инфраструктурах. Сущность этой задачи заключается в обосновании выбора показателей качества и метода (в рамках теории интервальных средних) оценки процесса реконфигурации схемы разграничения доступа в условиях динамично изменяющейся политики разграничения доступа. Предложены решения, позволяющие существенно повысить достоверность оценки качества алгоритма реконфигурации.

Введение. Проблема обеспечения разграничения доступа к информационным и телекоммуникационным ресурсам и защиты этих ресурсов, несмотря на имеющиеся в этой области научные и практические результаты, по-прежнему остается актуальной теоретической и практической задачей. В еще большей степени ее актуальность возрастает в случае интеграции разнородных ресурсов в облачных инфраструктурах критически важных информационных систем. Важнейшим из всех процессов, реализуемых в рамках этой проблемы, является процесс реконфигурации политик разграничения доступа (РПРД) [1].

При реализации процесса РПРД в облачных инфраструктурах критически важных информационных систем, ключевым вопросом теории и практики реконфигурации, ее обеспечения и текущего контроля, является математическое моделирование данного процесса, разработка алгоритмов и методов расчета, оценки и прогнозирования ее качества. Существующие подходы к решению задачи оценки качества процесса РПРД не универсальны, не учитывают целый ряд уникальных свойств, особенностей и динамики данного процесса, неполноту и неоднородность исходной информации о текущих значениях его показателей качества. Данное направление научно-практических исследований ориентировано на разработку новых методов расчета и многокритериального анализа качества процесса РПРД при неполной информации. Причем, оригинальность исследований состоит не только, и не столько, в создании современного методического и практического инструментария для анализа качества процессов такого класса, но и в сложности, многообразии и особых требованиях суперсистемы – облачной инфраструктуры критически важных информационных систем (КВИС).

Предлагаемый доклад посвящен рассмотрению общего подхода, сущности, особенностей и содержания этапов создания надежной методологической базы, позволяющей анализировать текущее состояние и качество процессов РПРД в интересах оптимального построения и управления ими для защиты ресурсов облачной инфраструктуры КВИС.

Актуальные вопросы разработки методики многокритериального анализа качества процесса реконфигурации политик разграничения доступа. Процесс РПРД представляет собой процедуру изменения существующей конфигурации связей между элементами (процедурами, механизмами) политики разграничения доступа к информационным ресурсам облачной инфраструктуры КВИС, выполняемую вручную или автоматически. Информационный ресурс облачной инфраструктуры КВИС – поименованная совокупность критически важных данных, хранимых и обрабатываемых в облачной инфраструктуре КВИС, к которой применяется политика (инструкции, методы, средства) обеспечения информационной безопасности.

Политика разграничения доступа в облачных инфраструктурах КВИС – совокупность документируемых административных (организационных), программно-аппаратных (физических) и юридических решений, а также набор правил, инструкций и ограничений (регламентов), однозначно и недвусмысленно определяющих (регламентирующих) все аспекты и саму модель контроля доступа – как процедурно-поведенческую модель деятельности должностных лиц и аппаратно-программных средств обеспечения информационной безопасности облачных инфраструктур КВИС в области разграничения доступа к ресурсам.

Помимо этого, существует ряд подходов к определению самого понятия «качество» любого процесса, включая процесс РПРД. Качество процесса – степень соответствия совокупности присущих характеристик процесса требованиям [2], Иногда говорят, что качество какого-либо процесса – это совокупность объективно присущих этому процессу свойств и характеристик, уровень или вариант которых формируется при определении цели процесса с целью удовлетворения существующих потребностей. Некоторые исследователи опираются на подход, изложенный в работе [3]: качество процесса – совокупность его свойств. В узком смысле и для нашего процесса – свойство или совокупность существенных свойств процесса РПРД, обуславливающих его соответствие назначению (цели).

Уникальность задачи анализа качества процесса РПРД обусловлена рядом причин.

Во-первых, повышение сложности процесса РПРД, наличие в его составе уникальных процедур всегда позволяют использовать традиционные методы анализа качества, основанные на применении теории вероятностей. Это связано либо с отсутствием, либо с недостаточностью исходной информации о динамике процесса РПРД.

Во-вторых, поскольку процесс РПРД является сложным процессом, то информация (данные) о его протекании и реализации для защиты ресурсов облачной инфраструктуры КВИС имеет различные источники. Отсюда возникает задача комбинирования разнородной по физической сущности информации о качестве процесса РПРД, получаемой по разным каналам.

В-третьих, информация может быть получена и в результате мониторинга процесса РПРД непосредственно, т.е., в ходе получения некоторого числа пошаговых динамических наблюдений от датчиков, сенсоров, активаторов и др. процесса РПРД. Но, по этим точечным наблюдаемым значениям нельзя построить достоверные прогностические вероятностные оценки.

В-четвертых, существующие подходы к анализу качества сложных процессов в динамике их реализации вынуждены, поочередно либо в комплексе, использовать пошаговые, математически и методологически сложные, громоздкие методы совместного использования нечетких множеств, искусственных нейронных сетей или нейро-нечетких (гибридных) сетей. Это позволяет повысить достоверность оценок, но при этом оценки будут получены точечные, пошаговые, что не всегда рационально. Зачастую предпочтительнее интервальные оценки качества процесса РПРД, усредненные за период наблюдения.

В-пятых, существующие отечественные стандарты оценки нацелены на контроль качества в определенных точках процесса РПРД и по показателям, не всегда соответствующих современным реалиям. Вместе с тем, известные международные стандарты, например, [4], приоритетные акценты расставляют на вопросах непрерывной оценки качества и анализа рисков на всех стадиях процесса РПРД. Это лишний раз подчеркивает важность и своевременность решения задачи разработки современного, строгого математического подхода, позволяющего комбинировать получаемую и имеющуюся информацию для вычисления общих интервальных оценок качества процесса РПРД. Это задача создания нового, удобного методологического инструмента поддержки принятия решений по управлению процессом РПРД.

Для того чтобы качественно защитить ресурсы облачной инфраструктуры КВИС, процесс РПРД должен быть высоко динамичным. Это связано с тем, что параметры угроз и самой облачной инфраструктуры КВИС постоянно изменяются. Даже при наличии необходимого объема статистических данных о значениях показателей качества процесса РПРД, редко наблюдается устойчивость этих значений во времени. Поэтому, либо нельзя определить точный закон распределения значений показателей качества (ПК) процесса РПРД и требуется рассматривать целый класс распределений, либо вообще нельзя определить ни закон, ни класс, а только некоторые частные ПК. К таким ПК процесса РПРД можно отнести численные значения параметров, например, характеризующих: устойчивость процесса РПРД – среднее время восстановления процесса после сбоя (нарушения) конфигурации; оперативность (своевременность реакции) – длительность промежутка времени от момента поступления запроса на реконфигурацию до момента окончания ее выполнения; непрерывность процесса РПРД – среднее время перерыва между окончанием предыдущего этапа процесса РПРД и началом следующего; скрытность (безопасность) процесса РПРД – среднее время вскрытия процессов протекающих в контуре управления РПРД [5].

Для многокритериального анализа качества процесса РПРД в интересах защиты ресурсов облачной инфраструктуры КВИС, в таких случаях целесообразно, на наш взгляд, использовать

интервальные статистические модели (с использованием известных положений теории интервальных средних), что требует разработки новых методов анализа и их обоснования.

Существующие методы анализа качества сложных управляемых процессов при неполной информации, основанные на использовании теории возможностей и теории нечетких множеств, являются разрозненными и решают ограниченные классы задач. Отсутствие общих, единых подходов к их применению на основе математической строгости, отсутствие обоснованной и практичной интерпретации всего многообразия ПК процессов, подобных процессу РПРД, затрудняет их применение в области контроля и управления безопасностью ресурсов облачных инфраструктур КВИС. Поэтому очень важной является задача не только разработки новых, современных, нетрадиционных подходов к анализу качества процесса РПРД, но и четкой и строгой аргументации их применения, установления связи с традиционными вероятностными ПК сложных процессов. Решение данных задач актуально в настоящее время, способно существенно повысить достоверность оценки качества алгоритма РПРД при расширении объемов и географии применения облачных инфраструктур КВИС, при построении новых высоконадежных их элементов, которые должны удовлетворять современным требованиям по безопасности.

Заключение. Таким образом, рассмотрены сущность и особенности нового подхода к решению задачи оценки качества процесса РПРД в критически важных облачных инфраструктурах при неполной информации. Данный подход основан на применении интервальных статистических моделей (в рамках теории интервальных средних). Предложены и обоснованы некоторые показатели качества процесса РПРД, их оценка в рамках методов теории интервальных средних дает более достоверные результаты анализа качества этого процесса. Возможным направления дальнейших исследований является синтез оптимального множества показателей качества обеспечения безопасности информации для облачных инфраструктур критически важных информационных систем.

Работа проводилась при поддержке гранта РФФИ № 18-07-01369

ЛИТЕРАТУРА

1. Shafig B., Vaidya J.S., Ghafoor A., Bertino E. A framework for verification and optimal reconfiguration of event-driven role based access control policies. *Publication in SACMAT`12: Proceedings of the 17th ACM symposium on Access Control Models and Technologies* (June 2012) P. 197–208.
2. Thoben K.D., Seifert M., Sitek P., Emde M., Tarditi R. Concept for Quality Control Management Services in Distributed Design Networks – Conceptual Paper. *Publication in IFIP International Federation for Information Processing*. vol. 257, Lean Business Systems and Beyond, Tomasz Koch, ed.; Boston: Springer, 2008. P. 461–471.
3. Mauch P.D. Quality management: theory and application. Boca Raton, FL: CRC Press, 2010. 143 p.
4. International Standard ISO/IEC/IEEE 15288:2015 «Systems and software engineering – System life cycle processes», NEQ. JTC 1/SC 7. 2015. 118 p.
5. Kolomeets M., Chechulin A., Kotenko I., Saenko I. Access control visualization using triangular matrices. *Publication in 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP).* IEEE. 2019. P. 348–355.

I.B. Parashchuk, I.B. Saenko (St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), St. Petersburg)

Assessment of the Quality of the Process of Reconfiguring Access Control Policies in Cloud Infrastructures of Critical Information Systems

Approaches to solving the problem of assessing the quality of the process of reconfiguring access control policies in critical cloud infrastructures are considered. The essence of this task is to substantiate the choice of quality indicators and the method (within the framework of the theory of interval averages) for assessing the process of reconfiguring an access control scheme under conditions of a dynamically changing access control policy. The solutions are proposed that allow to significantly increase the reliability of the quality assessment of the reconfiguration algorithm.