http://dx.doi.org/10.35596/1729-7648-2019-124-6-12-20

Оригинальная статья
Original paper

УДК 004.75

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ АНАЛИЗА МОДЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СИСТЕМ КЛАССА «ИНФРАСТРУКТУРА КАК УСЛУГА»

ОЛИЗАРОВИЧ Е.В., БРАЖУК А.И.

Гродненский государственный университет имени Янки Купалы, Республика Беларусь

Поступила в редакцию 3 мая 2018

Аннотация. Описан основанный на ролевом подходе процесс синтеза моделей информационной безопасности облачных компьютерных систем на основе прикладных моделей системы и угроз; результатом является модель защиты, выраженная, например, в рекомендациях по улучшению информационной безопасности или содержащая элементы конфигурации средств защиты. Предложена архитектура системы анализа моделей информационной безопасности облачных компьютерных систем, которая включает подсистему анализа и моделирования, базу знаний и подсистему интеграции с внешними источниками знаний. Система является ориентированной на модели (детальные, высокоуровневые, прикладные, синтезируемые) и предполагает автоматическую обработку знаний в сфере управления уязвимостями и настройки программного обеспечения. Предложен подход к решению задачи построения иерархий моделей архитектур и моделей угроз, реализующий комбинированный анализ функций и компонентов.

Ключевые слова: облачные компьютерные системы, инфраструктура как услуга, модель информационной безопасности.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Олизарович Е.В., Бражук А.И. Концептуальные основы анализа моделей информационной безопасности облачных систем класса «Инфраструктура как услуга». Доклады БГУИР. 2019; 6(124): 12-20.

CONCEPTUAL FRAMEWORK OF ANALYSIS OF INFORMATION SECURITY MODELS OF CLOUD SYSTEMS OF THE CLASS «INFRASTRUCTURE AS A SERVICE»

OLIZAROVICH E.V., BRAZHUK A.I.

Grodno State University named after Yanka Kupala, Republic of Belarus

Submitted 3 May 2018

Abstract. A process based on the role approach for the synthesis of information security models of cloud computing systems based on applied system and threat models is described; the result is a security model, expressed, for example, in recommendations for improving information security or containing elements

of the security configuration. The architecture of the system for analyzing models of information security of cloud computing systems is proposed. It includes a subsystem of analysis and modeling, a knowledge base and a subsystem of integration with external sources of knowledge. The system is model-oriented (detailed, high-level, applied, synthesized) and involves automatic processing of knowledge in the field of vulnerability management and software configuration. It is proposed an approach to solve the problem of constructing hierarchies of architectures models and threat models, realizing a combined analysis of functions and components.

Keywords: cloud computing systems, Infrastructure as a Service, IaaS, information security model.

Conflict of interests. The authors declare no conflict of interests.

For citation. Olizarovich E.V., Brazhuk A.I. Conceptual framework of analysis of information security models of cloud systems of the class «Infrastructure as a Service». Doklady BGUIR. 2019; 6(124): 12-20.

Введение

В настоящее время осуществляется активный переход предприятий с традиционной модели организации ИТ-инфраструктуры к облачной. Современные трансформации ИТ порождают множество проблем информационной безопасности, вызванных: потерей контроля над данными и использованием сети Интернет для их передачи; развитием мобильных систем и приложений, широким распространением вредоносного программного обеспечения и атак на основе социальной инженерии («спам», «фишинг», троянские программы); сложностью облачных систем, большим количеством их компонентов, различным административным подчинением компонентов и т. п.

Уровень «Инфраструктура как услуга» (Infrastructure as a Service – IaaS) является системообразующим для облачной инфраструктуры. Его технологическую основу составляют системы виртуализации, программно-определяемые сети (Software Defined Network – SDN) и хранилища (Software Defined Storage – SDS), а также современные модели использования ресурсов. Системообразующий характер и технологическая сложность требуют пристального исследования проблем информационной безопасности систем данного уровня [1]. Целью данной работы является разработка решений для анализа моделей информационной безопасности облачных компьютерных систем IaaS. Полученные результаты могут использоваться при проектировании систем защиты и анализе защищенности современных корпоративных информационных систем.

Основные определения

В рамках комплексного подхода обеспечение информационной безопасности должно осуществляться на организационном, процедурном и программно-техническом уровнях. При этом, независимо от уровня рассмотрения, основными инструментами описания предметной области являются архитектурные описания (архитектуры информационной безопасности, предметно-ориентированные модели защиты, архитектуры и модели средств защиты), а также модели процессов информационной безопасности (организационные процессы, документированные процедуры, автоматизированные и автоматические процессы).

Согласно [2], архитектуру системы составляют основные понятия и свойства системы в окружающей среде, воплощенные в ее элементах, отношениях и конкретных принципах ее развития. В общем виде разработка архитектуры системы связана с многоуровневой декомпозицией рассматриваемой проблемы и построением иерархической структуры системы.

Для управляемого использования архитектуры применяется комплексный рабочий продукт, который называется описанием архитектуры, основанный на точках зрения заинтересованных сторон и отражающий то или иное архитектурное представление. Наличие связей, определяющих отношения между компонентами, позволяет поддерживать все представления в согласованном состоянии и обеспечить целостность описания архитектуры.

Общепринятый подход к описанию процессов информационной безопасности базируется на защите активов (сущностей, имеющих субъективную ценность) [3]. Предполагается, что источники угроз (нарушители) хотят злоупотребить или нанести вред активам, порождая угрозы. Владельцы активов оценивают возможные угрозы и стремятся минимизировать риски информационной безопасности путем принятия определенных контрмер. Управление рисками обеспечивает идентификацию требований к защите информации в организации и создание эффективной системы менеджмента информационной безопасности.

Таким образом, основное предназначение предметно-ориентированных моделей информационной безопасности заключается в расширении и детализации риск-ориентированных моделей процессов обеспечения информационной безопасности при решении задач синтеза систем защиты и анализа защищенности облачных компьютерных систем. При этом рассматриваемые модели должны быть архитектурными моделями в терминах архитектурного описания, что обеспечивает их соответствие принципам, практикам и методологиям системной инженерии и архитектурного проектирования. Также модели должны быть совместимы с интерпретацией и терминологией, используемой в стандартах, литературе и реализациях средств информационной безопасности.

Архитектура системы анализа информационной безопасности

Обобщенный процесс синтеза модели защиты облачной компьютерной системы показан на рис. 1. Исходными данными являются прикладные модели: ролевые модели системы и модели угроз информационной безопасности. Каждая пара моделей (модель системы и модель угроз) создана данным потребителем (провайдер, разработчик, пользователь и т. п.) и отражает его точку зрения на проблему информационной безопасности целевой системы. Система анализа моделей информационной безопасности предназначена для дополнения («расширения») прикладных моделей до детального унифицированного представления, пригодного для автоматической обработки, а также для синтеза моделей защиты системы, соответствующих точкам зрения различных потребителей. На выходе данный потребитель получает модель защиты, которая отражает его представления и может быть выражена, например, в рекомендациях по улучшению системы защиты или элементах конфигурации компонентов облачной системы или средств защиты.

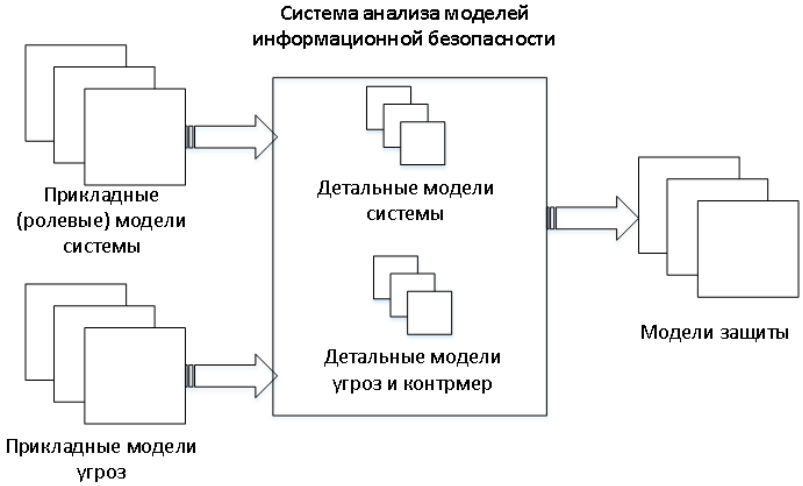

Рис. 1. Синтез модели информационной безопасности компьютерной системы
Fig. 1. Synthesis of a computer system information security model

Обобщенная архитектура системы анализа моделей информационной безопасности, показанная на рис. 2, включает три основных подсистемы: систему анализа и моделирования, базу знаний и подсистему интеграции с внешними источниками знаний.

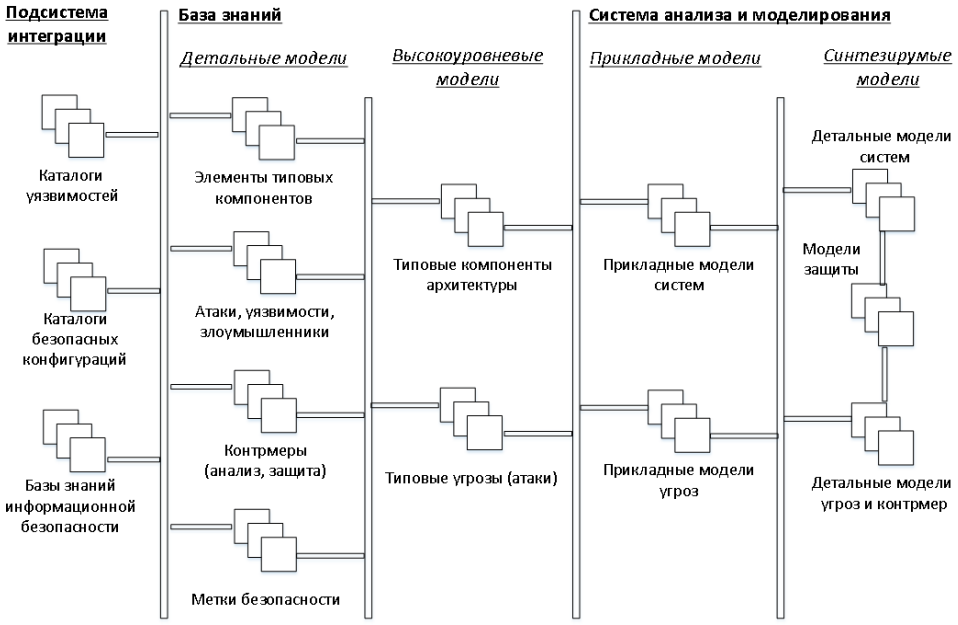

Рис. 2. Структура системы анализа моделей информационной безопасности
Fig. 2. The structure of the information security models analysis system

База знаний обеспечивает представление и обработку знаний предметной области и содержит два типа моделей.

1. Высокоуровневые модели. Представляют типовые компоненты и связи между ними, а также шаблоны архитектур компьютерных систем и атак (угроз), из которых потребители могут создавать прикладные модели, описывающие целевые системы.

2. Детальные модели. Включают списки и описания функциональных и структурных элементов типовых компонентов, атак, уязвимостей и злоумышленников, контрмер, которые обеспечивают анализ защищенности и непосредственно защиту. Используют метки безопасности, которые позволяют разделить понятия предметной области на большие классы (например, в соответствии с качественными характеристиками ущерба – конфиденциальность, целостность, доступность), что обеспечивает связь между моделями системы, а также предоставляет потребителю простые критерии оценки угроз.

Система анализа и моделирования оперирует двумя видами моделей.

1. Прикладные модели. Создаются потребителем на основе высокоуровневых моделей и служат исходными данными для моделирования.

2. Синтезируемые модели. Получаются путем анализа прикладных, высокоуровневых и детальных моделей; содержат детальные модели архитектур, а также угроз и контрмер для исследуемых систем; служат для синтеза моделей защиты.

Подсистема интеграции с внешними источниками знаний обеспечивает синхронизацию внешних баз знаний с базой знаний системы анализа. Эффективность данной подсистемы во многом определяет эффективность всей системы анализа, так как информационная безопасность является динамической сферой, и скорость получения и обработки новых знаний критически важна для ее обеспечения.

Предложенная архитектура, во-первых, является ориентированной на модели (т. е. оперирует формализованными представлениями архитектур, структур и процессов); во-вторых, предполагает функции автоматизированной и автоматической обработки знаний в области информационной безопасности. При этом основными проблемами реализации представленной системы анализа моделей информационной безопасности являются построение иерархий моделей архитектур (типовые компоненты –элементы типовых компонентов) и моделей угроз (типовые угрозы – атаки, уязвимости, злоумышленники, контрмеры, метки безопасности).

Моделирование облачных систем

Вопросы построения формальных моделей облачных компьютерных систем (в частности систем классов «Инфраструктура как услуга» и «Платформа как услуга») рассмотрены в исследованиях унифицированной онтологии облачных систем [4], построения онтологий для выбора облачных ресурсов [5], общей архитектуры облачной инфраструктуры на основе сервис-ориентированного подхода [6], унифицированной таксономии и архитектуры облачной среды [7], безопасных облачных технологий для критической инфраструктуры (проект SECCRIT, 2013 г.) [8]. Среди методов и технологий, которые могут быть использованы для формального описания, следует выделить методологию графического структурного анализа на основе диаграмм потоков данных DFD (Data Flow Diagram) [9], язык описания инфраструктуры и сети INDL (Infrastructure and Network Description Language) [10], а также подход, реализованный в общей информационной модели CIM (Common Information Model) [11].

Анализ вышеуказанных источников позволил сформулировать основные требования к исследуемым моделям. Формальная модель облачной компьютерной системы должна обеспечивать ее представление в виде набора программных компонентов и связей между этими компонентами. Абстракции компонентов и связей должны отражать существенные для задач обеспечения информационной безопасности особенности реальных элементов и способов их взаимодействия, а также поддерживать методы и технологии автоматической обработки данных и знаний. Однако следует отметить, что построение модели облачной системы затруднено ввиду архитектурных различий конкретных реализаций и недостатка информации о внутренней организации коммерческих систем [12].

В этих условиях предлагается использовать комбинированный подход, включающий следующее.

1. Анализ функций системы. Направлен на отражение уникальных особенностей и базируется на двухуровневой декомпозиции: выделение больших функциональных блоков системы и определение функций, связанных с каждым блоком.

2. Анализ компонентов системы. Определяет типовые особенности системы, что позволяет использовать для обеспечения информационной безопасности существующие теоретические и практические наработки. Компонент – некий типовой элемент архитектуры, который не отражает ее функционального назначения (например, современные информационные системы, независимо от их назначения, используют веб-приложения для взаимодействия с пользователями и СУБД для хранения и обработки данных).

Таким образом, процесс построения иерархии архитектурных моделей системы начинается с декомпозиции системы на относительно большие блоки (рис. 3), обособленные как с точки рассмотрения выполняемых функций, так и по составу компонентов. Далее каждый блок подвергается анализу на предмет выполняемых функций и компонентного состава. Анализ функций дает перечень (модель) функций для каждого блока, а анализ компонентов – перечень типовых компонентов. Входными данными для построения модели являются сведения об архитектурах различных облачных систем (описания структуры, состава, взаимосвязей и т. п.).

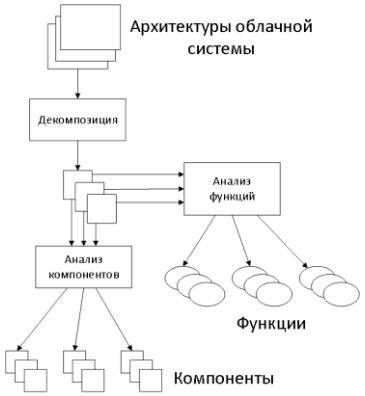

Рис. 3. Процесс построения иерархии архитектурных моделей
Fig. 3. The process of building a hierarchy of architectural models

Моделирование угроз облачных систем

Вопросы моделирования угроз облачных компьютерных систем (в частности систем класса IaaS) рассмотрены в исследованиях модели рисков для облачных технологий [13], численной модели влияния и оценки рисков облачной безопасности [14], эталонной онтологии операционной информации по кибербезопасности [15], а также в рамках проекта SECCRIT и др.

Анализ существующих моделей угроз облачных систем показал, что большинство моделей в той или иной степени реализуют классификационный подход, заключающийся в категоризации угроз информационной безопасности (по целям, источникам, уязвимостям, ущербам от реализации), информации (по важности, уровню конфиденциальности) и средств защиты (по функциональности). Данный подход широко используется на практике ввиду относительной простоты создания классификационной модели. При этом основным недостатком данного подхода является то, что результаты синтеза, как правило, сильно обобщены (не содержат рекомендации технического характера) и представляют совокупность средств защиты, а не целостную систему.

Реалистичная модель угроз облачной системы должна базироваться на моделях угроз (атак) компонентов, входящих в состав системы, причем декомпозиция функций системы позволяет выделить уникальные особенности системы с точки зрения информационной безопасности, декомпозиция компонентов – определить типовые элементы. Входными данными для построения типовых моделей угроз является совокупность возможных функциональных элементов и компонентов облачной системы. Типовая модель угроз соответствующего элемента включает перечень возможных угроз и их классификацию. Для связи с угрозами информационной безопасности, рассматриваемыми с точки зрения потребителя, элементы детальной классификации угроз должны быть снабжены «метками» соответствующих моделей.

Для построения актуальных моделей угроз необходима интеграция с внешними источниками знаний. С учетом больших объемов информации и необходимости высокой скорости ее обработки важное значение имеет автоматизация обработки данных в направлениях управления уязвимостями ПО и безопасной настройкой компонентов системы. Среди подходов, позволяющих обеспечить автоматизацию вышеуказанных процессов и автоматическую обработку данных следует выделить протокол автоматизации контента безопасности SCAP (Security Content Automation Protocol) института NIST (США) [16]. Протокол SCAP разработан для организации, представления и измерения информации по вопросам информационной безопасности. Он может использоваться для поддержания безопасности корпоративных систем, в частности, автоматической проверки установки обновлений, мониторинга настроек безопасности, анализа систем на признаки проникновения и т. п. Основу SCAP составляет язык OVAL (Open vulnerability and Assessment Language), который стандартизирует способы подачи информации, процесс анализа системы и формат выдаваемого результата.

Наиболее успешным элементом SCAP является словарь уязвимостей CVE (Common Vulnerabilities and Exposures), описывающий известные уязвимости в публично выпускаемом ПО. На основе CVE функционирует национальная база уязвимостей NVD (National Vulnerability Database), которая совместно со словарем программных продуктов CPE (Common Platform Enumeration) и системой оценок уязвимостей CVSS (Common Vulnerability Scoring System) составляет базис большинства средств управления уязвимостями, таких как CVESearch.com, Vulners.com, OpenVAS, Nessus.

Управление безопасностью конфигураций в SCAP обеспечивается расширяемым форматом описания контрольных листов настроек EXCCDF (Extensible Configuration Checklist Description Format), который позволяет формальные требования стандартов привязать к конкретным проверкам на защищаемой системе, описываемых OVAL. Однако данное направление проработано недостаточно, в частности, отсутствуют централизованная база безопасных настроек и средства анализа интеграции знаний в данной предметной области, что обуславливает исследовательский интерес к нему.

Заключение

Данная работа посвящена описанию концептуальных основ анализа моделей информационной безопасности облачных компьютерных систем класса IaaS. Полученные модели могут быть использованы при решении задач анализа защищенности облачных компьютерных систем, а также синтеза систем защиты.

В работе описан процесс синтеза моделей информационной безопасности облачных компьютерных систем на основе прикладных моделей системы и угроз, реализующий ролевой подход, а также предложена архитектура системы анализа моделей информационной безопасности облачных компьютерных систем. Структура системы включает подсистему анализа и моделирования, базу знаний и подсистему интеграции с внешними источниками знаний.

Основными преимуществами разработанной архитектуры являются: ориентация на модели (детальные модели, высокоуровневые модели, прикладные модели, синтезируемые модели), что позволяет применять широкий спектр методов и средств реализации моделей (семантический подход, имитационное моделирование, машинное обучение); включение функций автоматической обработки знаний по управлению уязвимостями и безопасными конфигурациями, что обеспечивает актуальность системы защиты.

Основными проблемами реализации представленной системы анализа моделей информационной безопасности являются построение иерархий моделей архитектур (типовые компоненты – элементы типовых компонентов) и моделей угроз (типовые угрозы – атаки, уязвимости, злоумышленники, контрмеры, метки безопасности). В рамках решения данных проблем предложен подход, реализующий комбинированный анализ функций и компонентов, а также приведен пример декомпозиции облачной системы класса IaaS.

Список литературы

1. Листопад Н.И., Олизарович Е.В., Бражук А.И. Практические аспекты внедрения облачных технологий в учреждении образования // Информатизация образования. 2014. № 2 (74). С. 55–65.
2. ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011. Системная и программная инженерия. Описание архитектуры.
3. СТБ 34.101.1-2014. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель.
4. Toward a unified ontology of cloud computing. / L. Youseff [et al.] // Grid Computing Environments Workshop. 2008. P. 1–10.
5. Moscato F., Di Martino B., Aversa R. Enabling model driven engineering of cloud services by using mosaic ontology //Scalable Computing: Practice and Experience. 2011. Vol. 13. №. 1. P. 29–44.
6. Intercloud architecture for interoperability and integration / Y. Demchenko [et al.] // Cloud Computing Technology and Science. 2012. P. 666–674.
7. Dukaric R., Juric M. Towards a unified taxonomy and architecture of cloud frameworks // Future Generation Computer Systems. 2013. Т. 29. №. 5. P. 1196–1210.
8. SEcure Cloud computing for CRitical infrastructure IT [Electronic resource]. URL: https://www.seccrit.eu/. (date of access: 20.04.2018).
9. Scandariato R., Wuyts K., Joosen W. A descriptive study of Microsoft's threat modeling technique // Requirements Engineering. 2015. Т. 20, №. 2. P. 163–180.
10. A semantic-web approach for modeling computing infrastructures / M. Ghijsen [et al.] // Computers & Electrical Engineering. 2013. № 39 (8). P. 2553–2565.
11. Common Information Model [Electronic resource]. / DMTF. URL: https://www.dmtf.org/standards/cim. (date of access: 20.04.2018).
12. Управление программным обеспечением и архитектура отказоустойчивого IaaS-облака на основе универсальных узлов. / Ю.И. Воротницкий [и др.] // Электроника ИНФО. 2013. № 9. С. 21–24.
13. Cloud Computing Risk Assessment [Electronic resource]. / ENISA, 2009. URL: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport. (date of access: 20.04.2018).
14. Saripalli P., Walters B. Quirc: A quantitative impact and risk assessment framework for cloud security // 2010 IEEE 3rd International Conference on Cloud Computing. 2010. P. 280–288.
15. Takahashi T., Kadobayashi Y. Reference ontology for cybersecurity operational information // The Computer Journal. 2014. Vol. 58, № 10. P. 2297–2312.
16. Security Content Automation Protocol [Electronic resource] / NIST. URL: https://csrc.nist.gov/projects/security-content-automation-protocol. (date of access: 20.04.2018).

References

1. Listopad N.I., Olizarovich E.V., Brazhuk A.I. Prakticheskie aspekty vnedrenija oblachnyh tehnologij v uchrezhdenii obrazovanija // Informatizacija obrazovanija. 2014. № 2 (74). S. 55–65. (in Russ.)
2. GOST R 57100-2016/ISO/IEC/IEEE 42010:2011. Sistemnaja i programmnaja inzhenerija. Opisanie arhitektury. (in Russ.)
3. STB 34.101.1-2014. Informacionnye tehnologii i bezopasnost'. Kriterii ocenki bezopasnosti informacionnyh tehnologij. Ch. 1. Vvedenie i obshhaja model'. (in Russ.)
4. Toward a unified ontology of cloud computing. / L. Youseff [et al.] // Grid Computing Environments Workshop. 2008. P. 1–10.
5. Moscato F., Di Martino B., Aversa R. Enabling model driven engineering of cloud services by using mosaic ontology //Scalable Computing: Practice and Experience. 2011. Vol. 13. №. 1. P. 29–44.
6. Intercloud architecture for interoperability and integration / Y. Demchenko [et al.] // Cloud Computing Technology and Science. 2012. P. 666–674.
7. Dukaric R., Juric M. Towards a unified taxonomy and architecture of cloud frameworks // Future Generation Computer Systems. 2013. T. 29. №. 5. P. 1196–1210.
8. SEcure Cloud computing for CRitical infrastructure IT [Electronic resource]. URL: https://www.seccrit.eu/. (date of access: 20.04.2018).
9. Scandariato R., Wuyts K., Joosen W. A descriptive study of Microsoft's threat modeling technique // Requirements Engineering. 2015. T. 20, №. 2. P. 163–180.
10. A semantic-web approach for modeling computing infrastructures / M. Ghijsen [et al.] // Computers & Electrical Engineering. 2013. № 39 (8). P. 2553–2565.
11. Common Information Model [Electronic resource]. / DMTF. URL: https://www.dmtf.org/standards/cim. (date of access: 20.04.2018).
12. Upravlenie programmnym obespecheniem i arhitektura otkazoustojchivogo IaaS-oblaka na osnove universal'nyh uzlov. / Ju.I. Vorotnickij [i dr.] // Jelektronika INFO. 2013. № 9. S. 21–24. (in Russ.)
13. Cloud Computing Risk Assessment [Electronic resource]. / ENISA, 2009. URL: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport. (date of access: 20.04.2018).
14. Saripalli P., Walters B. Quirc: A quantitative impact and risk assessment framework for cloud security // 2010 IEEE 3rd International Conference on Cloud Computing. 2010. P. 280–288.
15. Takahashi T., Kadobayashi Y. Reference ontology for cybersecurity operational information // The Computer Journal. 2014. Vol. 58, № 10. P. 2297–2312.
16. Security Content Automation Protocol [Electronic resource] / NIST. URL: https://csrc.nist.gov/projects/security-content-automation-protocol. (date of access: 20.04.2018).

Сведения об авторах

Олизарович Е.В., к.т.н., доцент, начальник Информационно-аналитического центра Гродненского государственного университета имени Янки Купалы.

Бражук А.И., ведущий инженер-программист Информационно-аналитического центра Гродненского государственного университета имени Янки Купалы.

Information about the authors

Olizarovich E.V., PhD, associate professor, head of the Information and Analytical Center of Grodno State University named after Yanka Kupala.

Brazhuk A.I., senior software engineer of the Information and Analytical Center of Grodno State University named after Yanka Kupala.

Адрес для корреспонденции

230023, Республика Беларусь,
г. Гродно, ул. Ожешко, 22
Гродненский государственный
университет имени Янки Купалы
тел: +375-152-72-01-44;
e-mail: brazhuk@grsu.by
Бражук Андрей Иосифович

Address for correspondence

230023, Republic of Belarus,
Grodno, Ozheshko str., 22
Grodno State University
named after Yanka Kupala
tel.: +375-152-72-01-44;
e-mail: brazhuk@grsu.by
Brazhuk Andrei Iosifovich