УДК 004.056
DOI: 10.15593/2224-9397/2020.4.10

С.Д. Волков, А.В. Царегородцев

Московский государственный лингвистический университет, Москва, Россия

ОДИН ИЗ ПОДХОДОВ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ АТАК ПРИ РЕАЛИЗАЦИИ ИНФОРМАЦИОННОЙ ФУНКЦИИ ГОСУДАРСТВА НА ВНУТРЕННЕМ УРОВНЕ

Возрастающая роль информационной сферы жизнедеятельности общества ставит перед государством задачу по работе в новом направлении деятельности – реализации информационной функции. Для реализации этой функции на внутреннем уровне, органами государственной власти создаются государственные информационные системы, используемые, в том числе, для обработки данных ограниченного доступа. В связи с этим, обеспечение информационной безопасности при обработке данных в таких системах приобретает немаловажное значение для государства. **Цель исследования:** противодействие угрозам целенаправленных атак на системы облачных вычислений на примере частной облачной среды. **Методы:** в данной статье предлагается подход к распознаванию атак на государственные информационные системы, основанный на методах функционального анализа, теории распознавания образов и использовании методов оценки рисков для снижения числа ложных срабатываний. **Результаты:** Предложен подход к обнаружению атак для частной облачной среды на основе теории распознавания образов. Атака представляется как образ, который необходимо распознать в ходе выполнения процессов накопления, обработки и передачи информации в гостевой операционной системе. Для выявления атаки необходимо установить вероятность соответствия определенному классу атак множества атак каждому объекту из множества атак на основе имеющегося описания и информации о классах атак. Затем можно использовать функции оценки близости (например, чебышевское расстояние) выявленного объекта атаки к известному классу атаки. В качестве дополнения к предложенному методу для снижения числа ложных срабатываний предлагается подход, основанный на методе оценки информационных рисков. Суть подхода заключается в том, что признаки атак ранжируются по уровню влияния определенных компонент. По каждому из критериев ранжирования для признака атаки устанавливается определенное количество баллов, оценивающее отнесения того или иного критерия к факту реализации атаки. Если сумма баллов превысит определенный порог, то можно говорить о выявлении атаки. **Практическая значимость:** полученные результаты могут быть использованы при создании систем обнаружения компьютерных атак в информационно-телекоммуникационных системах, функционирующих на основе технологии облачных вычислений, используемых при реализации информационной функции государства.

Ключевые слова: информационная функция государства, информационная безопасность, частная облачная среда, обнаружение компьютерных атак, система обнаружения вторжений, теория распознавания образов, оценка рисков.

S.D. Volkov, A.V. Tsaregorodtsev

Moscow State Linguistic University, Moscow, Russian Federation

ONE OF THE APPROACHES TO COMPUTER ATTACKS' RECOGNITION WHEN IMPLEMENTING THE STATE'S INFORMATION FUNCTION ON THE INTERNAL LEVEL

The growing impact of the information sphere on social life challenges the State with a new direction of activity - the implementation of the information function. To implement this function at the internal level, public authorities create state information systems that are used for processing sensitive data. Therefore ensuring information security when processing data in these systems becomes crucial for the state. **Purpose**: to counter targeted attacks on cloud computing based information systems on the example of private cloud environment. **Methods:** this study offers an approach to recognizing attacks on state information systems based on functional analysis methods, pattern recognition theory, and the use of risk assessment methods to reduce the number of false positives. **Results:** ат approach for attacks' recognition for private cloud environment based on the pattern recognition theory is proposed. The attack is presented as a pattern that must be recognized during the processes of storing, processing, and transferring information in the guest operating system. To detect an attack, it is necessary to determine the probability of matching a certain class of attacks of a set of attacks to each object from the set of attacks based on the available description and information about the attacks' classes. Then functions to estimate the proximity (for example, Chebyshev distance) of the detected attack object to a known attack class can be applied. In addition to the proposed method, an approach based on the information risk assessment is proposed to reduce the number of false positives. The essence of the approach is that the signs of attacks are ranked by the level of influence on certain components of an information system. Each of the ranking criteria is ranked with a certain number of points, which assesses whether a particular criterion is related to the fact of the attack implementation. If the sum of points exceeds a certain threshold, then a fact of attack recognition can be registered. **Practical relevance:** the results can be used to create intrusion detection systems for information and telecommunications systems, including those used when implementing the State's information function.

Keywords: state's information function, information security, private cloud environment, computer attack detection, intrusion detection system, pattern recognition theory, risk assessment.

Введение. Для современного этапа развития общества характерна все возрастающая роль информационной сферы, которая включает в себя как саму информацию и информационную инфраструктуру, так и субъектов, осуществляющих сбор, обработку, хранение, передачу и защиту информации. Государство при этом играет немаловажную роль в информационной сфере жизнедеятельности общества, реализуя тем самым соответствующее направление своей деятельности – информационную функцию государства [1].

Понятие информационной функции государства является одним из ключевых направлений его деятельности. В общем виде информационная функция государства – это комплекс мер, реализуемых государством для развития информационной сферы. В этот комплекс вхо-

дит совокупность общественных отношений, связанных с созданием, сбором, хранением, обработкой, передачей и защитой информации. Реализация информационной функции государства может включать в себя различные направления его деятельности – просвещение, декларацию, обеспечение, защиту, контроль и т.д.

Реализация любого из обозначенных направлений подразумевает информационный обмен между различными звеньями управленческой системы государства. А поскольку такой информационный обмен, как правило, включает в себя информацию ограниченного доступа, то обеспечение его безопасности приобретает немаловажное значение для государства. Более того, с возрастанием роли информационной сферы в жизнедеятельности общества это значение приобретает все более особую, если не первостепенную важность.

Особенности реализации информационной функции государства на внутреннем уровне. Реализация информационной функции государства на внутреннем уровне направлена на оптимизацию и повышение эффективности деятельности органов государственной власти. Сюда относится оптимизация внутренних информационных процессов государства, связанных со сбором, обработкой, хранением, передачей, засекречиванием и защитой информации [1].

В связи с возрастающей ролью информационной сферы, государством создаются государственные информационные системы [18], которые системы представляют собой особые объекты информационной инфраструктуры, поскольку создаются и эксплуатируются средствами и технологиями, сведения о которых государство не разглашает [15].

Одной из перспективных технологий для реализации информационной функции государства на внутреннем уровне является технология облачных вычислений.

«Облачные вычисления» (от английского «cloud computing») представляют собой одну из новых и наиболее активно развиваемых сетевых технологий [2, 9, 12].

Модель, предлагаемая Национальным институтом стандартов и технологий США (National Institute of Standards and Technology, NIST), дает следующее определение технологии «облачных вычислений»: это модель предоставления повсеместного удобного сетевого доступа «по требованию» к разделяемому пулу конфигурируемых вычислительных ресурсов (например, сети, серверы, память, приложения

и сервисы), которые могут быть предоставлены и освобождены в короткие сроки с минимальными усилиями в управлении или с минимальным взаимодействием с поставщиком услуги [16].

Модель выделяет три основных типа облачных сред: публичная, частная и гибридная облачная среда [3].

Принимая во внимание специфику реализации информационной функции государства на внутреннем уровне, наиболее оптимальным является использование частной модели развертывания облака [19, 20]. Это обусловлено следующими преимуществами частной модели [4, 13, 14]:

1) самостоятельное управление контролем доступа. Владелец облачной системы (орган государственной власти) сам определяет политику доступа к системе;

2) непрерывный мониторинг за доступностью имеющихся ресурсов с возможностью выделения дополнительных вычислительных мощностей в моменты пиковой нагрузки;

3) выделение отдельных каналов связи и особого приоритета в обслуживании для критичных сервисов;

4) возможность гибкого разграничения доступа в строгом соответствии с полномочиями пользователей с целью предотвращения несанкционированных потоков данных между пользователями и назначения минимальных привилегий.

К наиболее критичным недостаткам следует отнести [4, 13, 14]:

1) необходимость самостоятельной поддержки отказоустойчивости может оказаться сложной задачей, особенно при пиковых нагрузках;

2) обеспечение высокой доступности, избыточности и балансировки нагрузки требует дополнительных затрат;

3) истощение ресурсов может привести к снижению производительности и увеличению времени отклика облачных сервисов;

4) самостоятельный контроль информационной безопасности системы;

5) инсайдерские угрозы со стороны обслуживающего персонала.

Таким образом, использование частной облачной среды при реализации информационной функции государства на внутреннем уровне создает необходимость в поддержании ее доступности, а также в обеспечении конфиденциальности и целостности хранимых и обрабатываемых ею данных.

Проведенный анализ современного состояния исследований (работы В.А. Курбатова, П.Д. Зегжды, А.А. Грушо, Е.Е. Тимониной, В.Ю. Скибы, Н.А. Гайдамакина, А.А. Гладких, В.С. Заборовского и др.) позволяет сделать вывод о том, что [4, 7, 15]:

а) рост популярности информационно-телекоммуникационных систем, функционирующих на основе технологии облачных вычислений, способствует росту числа атак, направленных на них;

б) особую опасность для систем, построенных на основе технологии облачных вычислений, представляют направленные атаки, нарушающие правильное функционирование гипервизора и его подсистем;

в) отсутствуют отечественные научные и промышленные разработки (в том числе запатентованные), способные выявлять и противодействовать данному виду атак.

Совокупность данных фактов определяет научно-практическую проблему, на решение которой направлено данное исследование.

Целью исследования является противодействие угрозам целенаправленных атак на системы облачных вычислений на примере частной облачной среды, что впоследствии может быть использовано при создании систем обнаружения компьютерных атак в информационно-телекоммуникационных системах, функционирующих на основе технологии облачных вычислений, используемых при реализации информационной функции государства.

Основная идея подхода к обнаружению атак в частной облачной среде. Из результатов анализа архитектуры основных систем обнаружения компьютерных атак становится видно, что все они опираются на сигнатурный метод обнаружения атак и не адаптированы для полноценной работы в системах, функционирующих на основе технологии облачных вычислений [5, 6]. Наиболее опасными с точки зрения информационной безопасности облачной среды являются угрозы целенаправленных атак, которые нарушают функционирование подсистем гипервизора, отвечающих за планирование задач и верификацию команд на их соответствие требованиям информационной безопасности. Выявлять такие атаки и эффективно блокировать используемые ими каналы информационных воздействий сложно, так как эти каналы не доступны для контроля со стороны гостевых операционных систем. Критичность этих атак обусловливается также тем, что их реализация может нанести ущерб не только конкретному гостевому окружению, но и всей государственной информационной системе [5, 11].

Как уже излагалось, анализ современного состояния исследований в области информационной безопасности систем облачных вычислений свидетельствует о том, что вопрос противодействия угрозам целенаправленных атак на системы облачных вычислений вызывает все больший интерес, связанный с ростом их популярности и одновременным увеличением потока атак, ведущих к большим материальным потерям. Кроме того, в настоящее время отсутствуют системы обнаружения компьютерных атак, применимые в среде облачных вычислений.

Нами предлагается подход, основанный на методах функционального анализа и теории распознавания образов, в том числе с использованием обобщенного метода распознавания компьютерных атак [8].

Атака представляется как образ, который необходимо распознать в ходе выполнения процессов накопления, обработки и передачи информации в гостевой операционной системе:

$$M = \{\omega_1, \dots, \omega_n\},$$

где M – множество атак, ω_n – объекты атак.

Атаки и их признаки являются реализацией угроз информационной безопасности для облачной среды. ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» выделяет определенные типы угроз [9].

Объекты атак задаются соответствующими для них признаками – характеристиками, специфичными для каждой конкретной атаки:

$$x_i,\ i = 1, \dots, n.$$

Признаки атак могут представлять собой как логические переменные (истина/ложь), так и числовые значения, значения из набора возможных вариантов и т.д.

Пространство признаков атак формуется на основе имеющейся информации о функционировании гостевой операционной системы в облачной среде. По результатам испытаний метода в реальных условиях пространство признаков дополняется новыми признаками, полученными от имеющихся датчиков (сенсоров) системы обнаружения вторжений.

Совокупность признаков атак определяет описание каждого объекта атак ω_n множества атак M:

$$I(\omega_n) = \big(x_1(\omega_n),\ x_2(\omega_n), \dots, x_N(\omega_n)\big).$$

При этом на множестве атак M существует разбиение на подмножества (классы атак):

$$M = \bigcup_{i=0}^{m} \Omega_i.$$

Разбиение множества атак на классы может определяться некоторой априорной информацией I_0 о классах атак Ω_i (например, в соответствии с перечнем угроз в ГОСТ Р 56938-2016):

$$I_0(\Omega_1, \dots, \Omega_m).$$

Имея такую постановку задачи распознавания атаки, мы можем установить вероятность соответствия определенному классу атак множества атак M каждому объекту из множества атак ω на основе имеющегося описания $I(\omega)$ и информации I_0 о классах атак:

$$P_i = (\omega \in \Omega_i), \ \ i = 1, \dots, m.$$

Тогда множество возможных решений по противодействию выявленной атаке определяется как декомпозиция совокупности определенных признаков атак на области и установка их соответствия определенному классу:

$$\begin{cases} \forall \omega \in \Omega_i = \{\Omega_1, \dots, \Omega_m\}, \\ I_m \in I_0(\Omega_1, \dots, \Omega_m), \\ I(\omega_n) \in I(\omega), \ V_i \ \in \ V_n, \\ \exists P_i = (\omega \in \Omega_i), \ \ i = 1, \dots, m, \end{cases}$$

$$\forall x_i, \Omega_i = \{\Omega_1, \dots, \Omega_m\}, \exists F(x_i, \dots, x_n) \to \max,$$

где V_i – области на множестве признаков атак, $x_i, \dots, x_n$ – распознанные признаки атак, относящиеся к классу атак Ω_i, при которых функция распознавания F стремится к максимуму.

В качестве функции распознавания атак можно использовать функции оценки близости объекта атаки ω_n к классу атаки Ω_i. Одним из способов такой оценки является чебышевское расстояние:

$$d(X_i, X_j) = \max|x_{in} - x_{jn}|.$$

Однако недостаток этого метода заключается в том, что необходимо вручную определять как признаки атак x_i, так и их классы Ω_i и информацию о них I_0. В результате при недостаточном объеме этой информации будет иметь место относительно невысокий процент распознавания атак, а при избыточном – высокий процент ложных срабатываний.

В качестве одного из способов снижения количества ложных срабатываний можно рассмотреть подход, заключающийся в применении методов оценки информационных рисков [10, 11]. Суть подхода заключается в том, что признаки атак x_i ранжируются по уровню влияния следующих компонентов:

– возможных уязвимостей V_e конкретной облачной среды, существенных для реализации атаки (например, уязвимости в модуле фильтрации данных, вводимых пользователем);

– возможных вариантов реализации атаки S_e (например, использование различных подходов к эксплуатации потенциальной уязвимости в модуле фильтрации данных);

– индикаторов атаки Id_e (например, имена процессов, хэш-суммы, значения переменных и т.д.);

– симптомов реализации атаки Sy_e (например, появление соответствующих сообщений в журнале доступа при использовании автоматизированных средств поиска уязвимостей).

По каждому из критериев ранжирования для признака атаки устанавливается определенное количество баллов, оценивающее отнесения того или иного критерия к факту реализации атаки [17, 21].

Возможный ущерб от реализации атаки I_e можно определить как сумму данных компонентов:

$$I_e = \sum (V_e + S_e + Id_e + Sy_e).$$

Вероятность P_e проявления компонентов при реализации атаки определяется апостериорно в ходе настройки и испытания системы обнаружения вторжений в облачной среде.

Тогда, используя определение риска, можно дать оценку тому, что обнаруженные признаки атаки x_i действительно являются атакой, а не ложным срабатыванием:

$$R_a = \frac{1}{n} \sum P_e \cdot I_e,$$

где n – количество компонентов.

Если полученное значение R_a превышает определенный порог R_t, заданный в ходе настройки и испытания системы обнаружения вторжений в облачной среде, то можно говорить о том, что обнаруженные признаки атаки x_i являются атакой.

Исследование работы предлагаемого подхода к обнаружению атак в частной облачной среде. В качестве примера рассмотрим применение данного подхода для обнаружения атаки «внедрение SQL кода» (SQL-инъекция), осуществленной на СУБД, расположенную в облачной среде. Для каждого признака атаки x_i необходимо задать вероятность проявления каждого из компонентов V_e, S_e, Id_e, Sy_e и величину возможного ущерба от ее проявления в баллах (таблица) [10]. Данные значения определяются на основе имеющихся знаний о конкретной системе в ходе настройки и испытаний системы обнаружения вторжений. Также необходимо задать пороговое значение R_t, при превышении которого выявленные признаки атаки x_i регистрируются как атака.

Оценка риска реализации атаки «внедрение SQL кода»

Компонент	Вероятность (x_1)	Вероятность (x_2)	Ущерб (x_1)	Ущерб (x_2)	$R_a(x_1)$	$R_a(x_2)$
V_e	1	3	3	1	3	3
S_e	3	2	4	3	12	6
Id_e	2	2	4	3	8	6
Sy_e	2	3	4	1	8	3
Оценка риска					7,75	4,5

Таким образом, к примеру, при, $R_t = 6$, при выявлении в потоке данных только одного признака атаки x_2 система не зарегистрирует атаку и продолжит функционирование в штатном режиме.

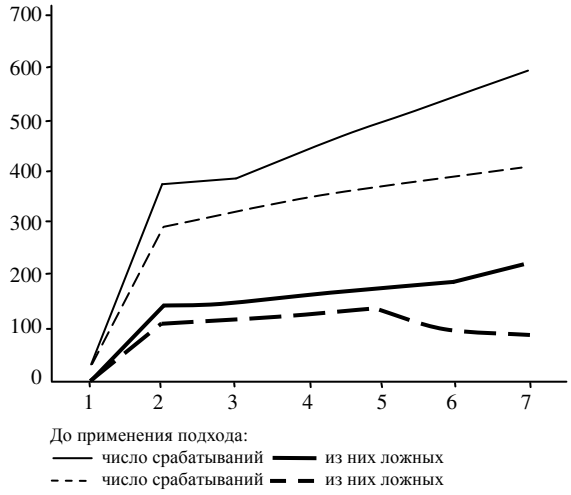


Рис. Эффективность обнаружения атак до и после применения подхода, основанного на оценке информационных рисков

На рисунке показано сравнение числа ложных срабатываний системы при обнаружении атак для вышеуказанного примера «внедрения SQL-кода» (SQL-инъекции) на СУБД, расположенной в облачной среде.

Из рисунка видно, что после применения подхода, основанного на оценке информационных рисков, число ложных срабатываний снизилось в среднем на 10–15 %.

Выводы. В статье рассмотрены вопросы реализации информационной функции государства, которая на внутреннем уровне включает создание государственных информационных систем, используемых, кроме прочего, для сбора, обработки и хранения информации ограниченного доступа. Применение модели развертывания частной облачной среды для создания государственных информационных систем является одним их подходов к оптимизации и повышению эффективности деятельности органов государственной власти. Поскольку специфические характеристики среды облачных вычислений усложняют внедрение системы обнаружения вторжений из-за высокого количества ложных срабатываний, рассмотрена необходимость в разработке нового подхода к обнаружению, анализу и противодействию вредоносным воздействиям на облачные среды.

Предложенный способ обнаружения атак для частной облачной среды на основе теории распознавания образов и использования методов оценки рисков для снижения числа ложных срабатываний в ряде случаев позволяет эффективно решать данную проблему. Проведенные эксперименты показывают, что использование методов оценки риска позволяет уменьшить число ложных срабатываний в среднем на 10–15 %. Отсутствие отечественных научных и промышленных разработок (в том числе запатентованных), способных выявлять и противодействовать направленным атакам, нарушающим правильное функционирование гипервизора и его подсистем, позволяет говорить о новизне данного исследования.

Стоит учесть, что предложенный метод зависит от степени детализации распознавания атак, которая напрямую зависит от количества классов распознавания атак и количества возможных решений по противодействию им. Дальнейшие исследования данного вопроса могут быть направлены на поиск более универсальных способов описания признаков атак, исследование подходов к созданию баз данных признаков, поиск новых способов уменьшения числа ложных срабатываний. Полученные

в ходе данного и возможных будущих исследований результаты могут быть использованы при создании систем обнаружения компьютерных атак в информационно-телекоммуникационных системах, функционирующих, кроме прочего, на основе технологии облачных вычислений и используемых при реализации информационной функции государства.

Библиографический список

1. Околёснова О.А. Обеспечение информационной безопасности в рамках реализации информационной функции государства // Информационное пространство: обеспечение информационной безопасности и право: сб. науч. трудов / под ред. Т.А. Поляковой, В.Б. Наумова, А.В. Минбалеева. – М.: Изд-во ИГП РАН, 2018. – С. 304–308.

2. Царегородцев А.В., Качко А.К. Обеспечение информационной безопасности на облачной архитектуре организации // Национальная безопасность. – М.: НБ Медиа, 2011. – № 5. – С. 25–34.

3. The NIST Definition of Cloud Computing [Электронный ресурс]. – URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (дата обращения: 15.05.2020).

4. Царегородцев А.В. SWOT-анализ информационной безопасности корпоративных систем на основе облачных вычислений // Новые информационные технологии: тез. докл. XX Междунар. студенческой конф.-школы-семинара. – М.: Изд-во МИЭМ, 2012. – 416 с.

5. Волков С.Д. Обзор подходов к построению систем обнаружения компьютерных атак для информационно-телекоммуникационных систем, функционирующих на основе технологии облачных вычислений // Collegium Linguisticum-2017: материалы ежегодной конф. студ. науч. общества МГЛУ. – М.: Изд-во МГЛУ, 2017. – С. 442–447.

6. Гамаюнов Д.Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов: дис. – М.: Изд-во МГУ, 2007.

7. Волков С.Д. Нейросетевая система обнаружения вторжений в информационно-телекоммуникационные системы, функционирующие на основе технологии облачных вычислений: выпускная квалификационная работа (магистер. дис.) / Моск. гос. лингвист. ун-т. – М., 2017.

8. Климов С.М. Методы и модели противодействия компьютерным атакам. – Люберцы: КАТАЛИТ, 2008. – 316 с.

9. ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения.

[Электронный ресурс]. – URL: http://docs.cntd.ru/document/1200135524 (дата обращения: 15.05.2020).

10. Intrusion detection in cloud computing based attack patterns and risk assessment / B.C. Youssef, M. Nada, B. Elmehdi, R. Boubker // Advances in Science, Technology and Engineering Systems Journal. – 2017. – Vol. 2, № 3. – С. 479–484.

11. Царегородцев А.В., Савельев И.А., Мухин И.Н. Один из подходов анализа рисков безопасности данных в облачных средах // Современная наука: актуальные проблемы теории и практики. Сер. Естественные и технические науки. – М.: Научные технологии, 2014. – № 1–2. – С. 57–65.

12. Царегородцев А.В., Мухин И.Н. Синтез развивающихся информационно-управляющих систем // Автоматизация и современные технологии. – М.: Машиностроение, 2004. – № 11. – С. 12–21.

13. Мухин И.Н. Анализ рисков управления информационной безопасностью предприятия как этап комплексной защиты объектов информатизации // Современная наука: актуальные проблемы теории и практики. Сер. Естественные и технические науки. – М., 2012. – № 4/5. – С. 33–37.

14. Царегородцев А.В., Мухин И.Н., Белый А.Ф. Методика построения защищенных информационно-телекоммуникационных систем на базе гибридной облачной среды // Информация и безопасность. – Воронеж: Изд-во ВГТУ, 2015. – Т. 18, № 3. – С. 404–407.

15. Царегородцев А.В., Мухин И.Н., Боридько С.И. Один из подходов к построению информационной инфраструктуры организации на базе гибридной облачной среды // Информация и безопасность. – Воронеж: Изд-во ВГТУ, 2015. – Т. 18. – № 3. – С. 400–403.

16. Information security management for cloud infrastructure / A.V. Tsaregorodotsev, I.Ya. Lvovich, M.S. Shikhaliev, A.N. Zelenina, O.N. Choporov // International Journal on Information Technologies and Security. – 2019. – Vol. 11, No. 3. – P. 91–100.

17. Information security risk estimation for cloud infrastructure / A.V. Tsaregorodtsev, O.Ja. Kravets, O.N. Choporov, A.N. Zelenina // International journal on information technologies and security. – 2018. – Vol. 10, No. 4. – P. 64–76.

18. Царегородцев А.В., Тараскин М.М. Методы и средства защиты информации в государственном управлении: учеб. пособие. – М.: Проспект, 2017. – 193 с.

19. Царегородцев А.В., Макаренко Е.В. Оценка уязвимостей для различных типов развертывания облачных сред // Безопасность информационных технологий. – 2014. – № 4. – С. 112–117.

20. Tsaregorodtsev A., Zelenina A., Ružický E. Methodology of vulnerability assessment for various types of cloud structures // Information Technology Applications. – Bratislava, Slovakia, 2017. – No. 1. – P. 51–60.

21. Царегородцев А.В., Зеленина А.Н., Савельев В.А. Классификация уязвимостей облачных сред в задаче количественной оценки риска // Моделирование, оптимизация и информационные технологии. – Воронеж: Изд-во Воронеж. ин-та высоких технол., 2017. – № 4(19). – С. 38.

References

1. Okolesnova O.A. Obespechenie informatsionnoi bezopasnosti v ramkakh realizatsii informatsionnoi funktsii gosudarstva [Ensuring information security as part of the implementation of the information function of the state]. *Informatsionnoe prostranstvo: obespechenie informatsionnoi bezopasnosti i pravo. Sbornik nauchnykh trudov*. Eds. T.A. Poliakova, V.B. Naumov, A.V. Minbaleev. Moscow: Institut gosudarstva i prava Rossiiskoi akademii nauk, 2018, pp. 304-308.

2. Tsaregorodtsev A.V., Kachko A.K. Obespechenie informatsionnoi bezopasnosti na oblachnoi arkhitekture organizatsii [Providing information security on the cloud architecture of the organization]. *Natsional'naia bezopasnost'*. Moscow: NB Media, 2011, no. 5, pp. 25-34.

3. The NIST Definition of Cloud Computing, available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (accessed 15 May 2020).

4. Tsaregorodtsev A.V. SWOT-analiz informatsionnoi bezopasnosti korporativnykh sistem na osnove oblachnykh vychislenii [SWOT analysis of information security of corporate systems based on cloud computing]. *Novye informatsionnye tekhnologii. Tezisy dokladov KhX Mezhdunarodnoi studencheskoi konferentsii-shkoly-seminara*. Moscow: Moskovskii institut elektroniki i matematiki, 2012, 416 p.

5. Volkov S.D. Obzor podkhodov k postroeniiu sistem obnaruzheniia komp'iuternykh atak dlia informatsionno-telekommunikatsionnykh sistem, funktsioniruiushchikh na osnove tekhnologii oblachnykh vychislenii [A review of approaches to the construction of computer attack detection systems

for information and telecommunications systems operating on the basis of cloud computing technology]. *Collegium Linguisticum-2017. Materialy ezhegodnoi konferentsii studentov nauchnogo obshchestva MGLU*. Moscow: Moskovskii gosudarstvennyi lingvisticheskii universitet, 2017, pp. 442-447.

6. Gamaiunov D.Iu. Obnaruzhenie komp'iuternykh atak na osnove analiza povedeniia setevykh ob"ektov [Detection of computer attacks based on the analysis of the behavior of network objects]. Ph. D. thesis. Moscow: Moskovskii gosudarstvennyi universitet, 2007.

7. Volkov S.D. Neirosetevaia sistema obnaruzheniia vtorzhenii v informatsionno-telekommunikatsionnye sistemy, funktsioniruiushchie na osnove tekhnologii oblachnykh vychislenii: vypusknaia kvalifikatsionnaia rabota [Neural network intrusion detection system for information and telecommunications systems operating on the basis of cloud computing technology]. Master's thesis. Moscow: Moskovskii gosudarstvennyi lingvisticheskii universitet, 2017.

8. Klimov S.M. Metody i modeli protivodeistviia komp'iuternym atakam [Methods and models for countering computer attacks]. Liubertsy: KATALIT, 2008, 316 p.

9. GOST R 56938-2016. Zashchita informatsii. Zashchita informatsii pri ispol'zovanii tekhnologii virtualizatsii. Obshchie polozheniia [GOST R 56938-2016. Information protection. Protect information with virtualization technologies. General provisions], available at http://docs.cntd.ru/document/1200135524 (accessed 15 May 2020).

10. Youssef B.C., Nada M., Elmehdi B., Boubker R. Intrusion detection in cloud computing based attack patterns and risk assessment. *Advances in Science, Technology and Engineering Systems Journal*, 2017, vol. 2, no. 3, pp. 479-484.

11. Tsaregorodtsev A.V., Savel'ev I.A., Mukhin I.N. Odin iz podkhodov analiza riskov bezopasnosti dannykh v oblachnykh sredakh [One approach to analyzing data security risks in cloud environments]. *Sovremennaia nauka: aktual'nye problemy teorii i praktiki. Estestvennye i tekhnicheskie nauki*. Moscow: Nauchnye tekhnologii, 2014, № 1-2, pp. 57-65.

12. Tsaregorodtsev A.V., Mukhin I.N. Sintez razvivaiushchikhsia informatsionno-upravliaiushchikh sistem [Synthesis of developing information and control systems]. *Avtomatizatsiia i sovremennye tekhnologii*. Moscow: Mashinostroenie, 2004, no. 11, pp. 12-21.

13. Mukhin I.N. Analiz riskov upravleniia informatsionnoi bezopasnost'iu predpriiatiia kak etap kompleksnoi zashchity ob"ektov informatizatsii [Analysis of risks of enterprise information security management as a stage of complex protection of informatization objects]. *Sovremennaia nauka: aktual'nye problemy teorii i praktiki. Estestvennye i tekhnicheskie nauki*. Moscow, 2012, no. 4/5, pp. 33-37.

14. Tsaregorodtsev A.V., Mukhin I.N., Belyi A.F. Metodika postroeniia zashchishchennykh informatsionno-telekommunikatsionnykh sistem na baze gibridnoi oblachnoi sredy [How to build secure information and telecommunications systems based on hybrid cloud]. *Informatsiia i bezopasnost'*. Voronezh: Voronezhskii gosudarstvennyi tekhnicheskii universitet, 2015, vol. 18, no. 3, pp. 404-407.

15. Tsaregorodtsev A.V., Mukhin I.N., Borid'ko S.I. Odin iz podkhodov k postroeniiu informatsionnoi infrastruktury organizatsii na baze gibridnoi oblachnoi sredy [One approach to building your organization's information infrastructure from a hybrid cloud]. *Informatsiia i bezopasnost'*. Voronezh: Voronezhskii gosudarstvennyi tekhnicheskii universitet, 2015, vol. 18, no. 3, pp. 400-403.

16. Tsaregorodotsev A.V. Lvovich I.Ya., Shikhaliev M.S., Zelenina A.N., Choporov O.N. Information security management for cloud infrastructure. *International Journal on Information Technologies and Security*, 2019, vol. 11, no. 3, pp. 91-100.

17. Tsaregorodtsev A.V., Kravets O.Ja., Choporov O.N., Zelenina A.N. Information security risk estimation for cloud infrastructure. *International journal on information technologies and security*, 2018, vol. 10, no. 4, pp. 64-76.

18. Tsaregorodtsev A.V., Taraskin M.M. Metody i sredstva zashchity informatsii v gosudarstvennom upravlenii [Methods and means of information protection in public administration]. Moscow: Prospekt, 2017, 193 p.

19. Tsaregorodtsev A.V., Makarenko E.V. Otsenka uiazvimostei dlia razlichnykh tipov razvertyvaniia oblachnykh sred [Vulnerability assessment for different types of cloud deployments]. *Bezopasnost' informatsionnykh tekhnologii*, 2014, no. 4, pp. 112-117.

20. Tsaregorodtsev A., Zelenina A., Ružický E. Methodology of vulnerability assessment for various types of cloud structures. *Information Technology Applications*. Bratislava, Slovakia, 2017, no. 1, pp. 51-60.

21. Tsaregorodtsev A.V., Zelenina A.N., Savel'ev V.A. Klassifikatsiia uiazvimostei oblachnykh sred v zadache kolichestvennoi otsenki riska [Classifying cloud vulnerabilities in risk quantification]. *Modeling, optimization and information technology*. Voronezh: Voronezhskii institut vysokikh tekhnologii, 2017, no. 4(19), 38 p.

Сведения об авторах

Волков Сергей Дмитриевич (Москва, Россия) – аспирант кафедры «Международная информационная безопасность» Московского государственного лингвистического университета (119034, Москва, ул. Остоженка, 38/1, e-mail: volkov1234@gmail.com).

Царегородцев Анатолий Валерьевич (Москва, Россия) – профессор кафедры «Международная информационная безопасность» Московского государственного лингвистического университета (119034, Москва, ул. Остоженка, 38/1, e-mail: avtsaregorodtsev@linguanet.ru).

About the authors

Volkov Sergey Dmitrievich (Moscow, Russian Federation) is a Graduate Student Department of International Information Security Moscow State Linguistic University (119034, Moscow, 38/1, Ostozhenka str., e-mail: volkov1234@gmail.com).

Tsaregorodtsev Anatoliy Valeryevich (Moscow, Russian Federation) is a Doctor of Technical Sciences, Professor Department of International Information Security Moscow State Linguistic University (119034, Moscow, 38/1, Ostozhenka str., e-mail: avtsaregorodtsev@linguanet.ru).

Получено 07.10.2020