Описание взаимодействий различных метрик системы при использовании методики определения угроз информационной безопасности инстансов облачной инфраструктуры, основанной на теории графов

Пестов Игорь Евгеньевич
кандидат технических наук, доцент кафедры ЗСС Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, ip@sut.ru

Федоров Павел Олегович
аспирант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия, pavel_lenin@mail.ru

Федорова Екатерина Сергеевна
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия, ek.chukina@yandex.ru

Смуров Илья Александрович
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия, ismurov@mail.ru

АННОТАЦИЯ

Введение: В данной работе рассматривается проблема информационной безопасности инстансов облачной инфраструктуры**. Цель исследования**: В приведенной работе было необходимо описать взаимодействий различных метрик системы при использовании методики определения угроз информационной безопасности инстансов облачной инфраструктуры, основанной на теории графов. **Результаты**: Приведено описание взаимодействий различных параметров системы, используемое для построения графа состояния системы. Описание данных взаимодействий способствуют более детальному анализу состояния системы при реализации различных угроз информационной безопасности злоумышленником. В статье приведены конкретные примеры изменения метрик облачной инфраструктуры, характерные для таких типов угроз как атака «отказ в обслуживании» и атака вируса майнера. **Практическая значимость:** данный метод позволяет повысить эффективность определения угроз информационной безопасности инстансов облачной инфраструктуры. **Обсуждение:** в качестве дальнейшего исследования требуется детальное рассмотрение аномалий во взаимодействие различных метрик облачной инфраструктуре, характерных для неизвестных типов угроз.

КЛЮЧЕВЫЕ СЛОВА: облачная инфраструктура; информационная безопасность; метрика; инстанс; виртуальная машина; контейнер.

Введение

Стремительное развитие технологий виртуализации и создание сред облачных вычислений формирует новые источники угроз, которые необходимо учитывать при обеспечении информационной безопасности современных компьютерных систем и сервисов. При этом динамический характер процессов информационного взаимодействия существенно затрудняет возможности оперативной оценки рисков нарушения конфиденциальности, целостности и доступности программных и инфраструктурных ресурсов, предоставляемых в режиме удаленного доступа. Традиционные средства обеспечения информационной безопасности такие как средства разграничения доступа, межсетевые экраны, системы обнаружения вторжений контролируют только те информационные потоки, которые проходят по каналам, предназначенным для их передачи, поэтому угрозы, реализуемые посредством скрытых каналов передачи информации, с их помощью не могут быть блокированы. В этих условиях важное значение приобретают технологии защиты от угроз, которые формируются с использованием скрытых каналов информационного воздействия или внутри периметра безопасности корпоративной компьютерной сети. Защита от таких деструктивных воздействий требует создания новых моделей и методов противодействия попыткам внешних и внутренних пользователей изменить состояние защищенности информационных ресурсов среды облачных вычислений.

Описание взаимодействий различных метрик системы при использовании методики определения угроз информационной безопасности инстансов облачной инфраструктуры, основанной на теории графов.

Эффективным средством обнаружения нарушений периметра безопасности облачных инфраструктур является методика обнаружения угроз информационной безопасности инстансов облачной инфраструктуры основанная на теории графов. Данная методика базируется на анализе графа состояния инстансов облачной инфраструктуры. Построение графа состояния осуществляется из метрик состояния получаемых от соответствующего модуля сбора в облачной инфраструктуре в рамках набора параметров, которые соответствуют аномалии. Собранные метрики формируют массив вершин ориентированного графа, а в качестве ребер выступают взаимодействия между метриками одного типа, а также взаимосвязи метрик различного вида.

Методика определения угроз информационной безопасности инстансов облачной инфраструктуры, основанная на теории графов, включает в себя использование различных метрик системы для анализа и оценки уровня угроз. Суть методики заключается в определении конкретного типа угрозы нарушения информационной безопасности инстансов облачной инфраструктуры посредством анализа графа состояния. Граф анализируется путем работы алгоритмов обхода в ширину и в глубину, с целью выявления аномального состояния метрик. При анализе графа состояния инстансов облачной инфраструктуры важно использовать различные метрики для получения более полной картины о текущем состоянии системы. Некоторыми из основных метрик, которые могут использоваться в данном анализе, являются:0

1. Пропускная способность сети: метрика, которая оценивает скорость передачи данных между инстансами. Она может использоваться для определения узких мест и проблем с производительностью.

2. Загрузка ЦПУ: метрика, которая измеряет процент использования процессора на различных инстансах. Она может помочь определить, используется ли вычислительная мощность эффективно и оптимально.

3. Загрузка диска: метрика, которая показывает, насколько загружен диск на инстансе. Она может помочь выявить проблемы с доступом к данным и оптимизировать производительность.

4. Доступность: метрика, которая отслеживает время доступности инстансов. Она может использоваться для определения уровня надежности и стабильности облачной инфраструктуры.

При анализе графа состояния инстансов облачной инфраструктуры эти метрики могут взаимодействовать между собой, например, высокая загрузка ЦПУ может привести к увеличению времени доступности или уменьшению пропускной способности сети. Понимание взаимосвязи между этими метриками позволяет выявлять проблемы и оптимизировать работу системы. Анализируя взаимодействия различных метрик между собой и выявив отклонения от нормального состояния этих смежных метрик, можно определить конкретный маркер того или иного типа угрозы с высокой степенью точности. Это обусловлено тем что для конкретного типа угрозы, характерны определенные изменения в параметрах системы. После определения типа угрозы, описываемая методика подразумевает автоматизированное применения мер противодействия.

На первом этапе работы методики необходимо выделить несколько параметров, на которых будет основываться проведение анализа стабильности работы информационной системы. В анализе участвуют параметры: RAM, CPU, Storage, Network.

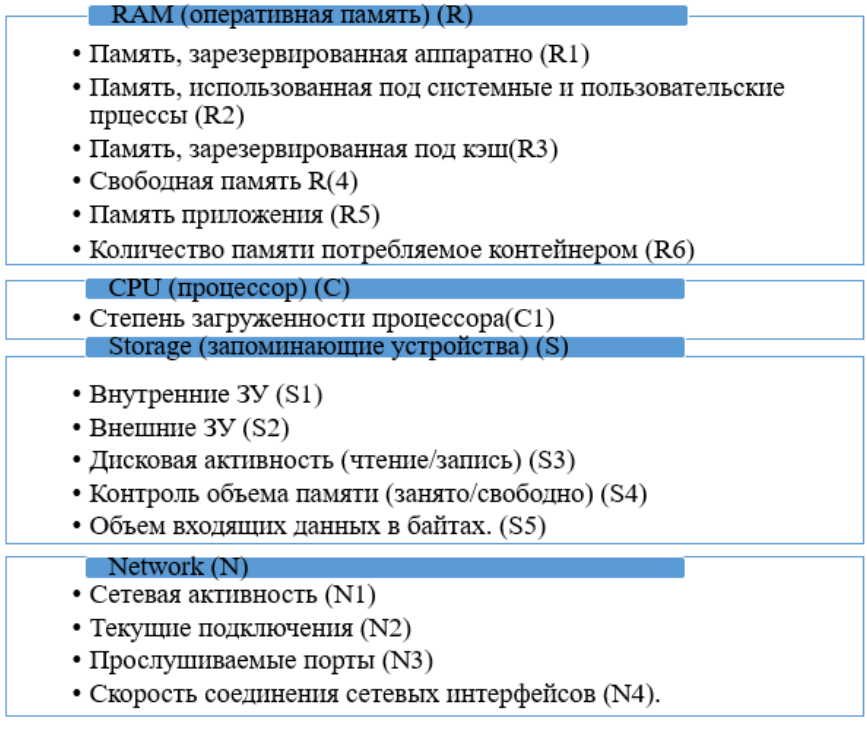

Рис.1. Параметры и характеристики, выделенные для оценки состояния системы.

Для реализации методики принятия решений, за основу принимается метод весовых коэффициентов. При экспериментальной проверке анализ стабильности работы информационной системы основывается на параметрах, которые отображены на рисунке 1, каждый из них включает определенные характеристики (коэффициенты). В конечном итоге, выделено шестьнадцать коэффициентов, основываясь на которых можно провести анализ состояния системы. Оценочные значения каждому коэффициенту присваиваются по следующему правилу: состояние параметра системы определяется по двоичной системе, в которой 0 – допустимое значение параметра, 1 – значение, которое отличается от задаваемого при стабильной работе системы. Анализируя состояние системы при её нестабильной работе, сначала нужно определить параметр, а в дальнейшем – коэффициент, значение которого обуславливает нестабильность работы.

Чтобы определить наилучшее средство противодействия угрозам нарушения информационной безопасности используется теория графов. Для этого по представленным выше метрикам строится граф состояния. Рассматриваемой системы. Пример графа состояния представлен на рисунке 2.

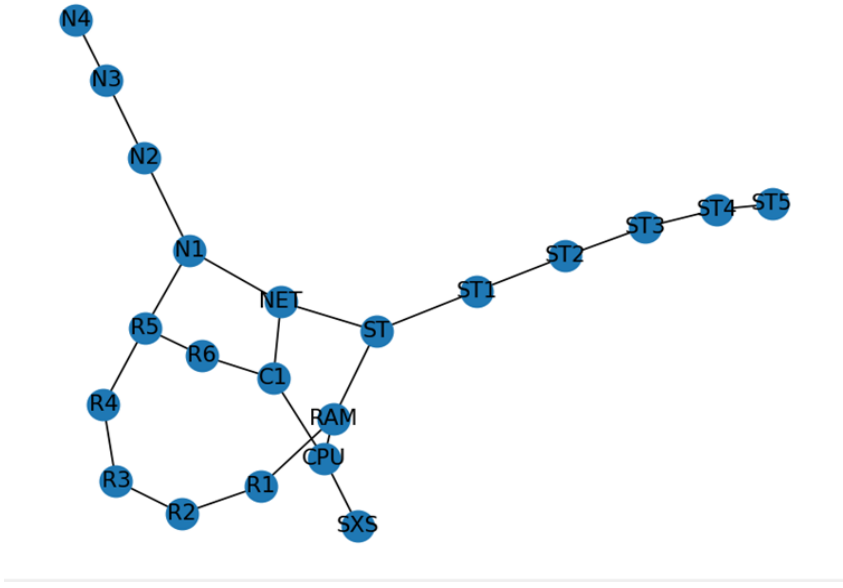

Рис.2. Граф состояния системы.

Данный граф можно быть описан следующим образом (1):

$$SYS = K_1 \cup K_2 \cup K_3 \cup \ldots \cup K_n \quad (1)$$

где K – выделенный параметр, n – общее число параметров.

При этом (2):

$$K_i = k_1 \cup k_2 \cup k_3 \cup \ldots \cup k_x, \quad (2)$$

где ki – характеристика параметра, x – общее число характеристик параметра.

Построение графа состояния облачной инфраструктуры по данным параметрам позволяет наглядно описать их взаимодействие. К примеру, от памяти используемых приложений (R5) напрямую зависит сетевая активность (N1), а от количества памяти потребляемое контейнерами, входящими в облачную инфраструктуру (R6) а также от памяти приложений (R5) зависит степень загруженности процессора (C1) на которую также влияет общая сетевая активность (NET).

Для более точечного анализа взаимодействий различных метрик между собой для данного графа состояния необходимо сформировать матрицу смежности. Матрица смежности является математическим отображением смежности вершин графа, т.е. взаимосвязи метрик инстансов облачной инфраструктуры между собой. Построение данной матрицы позволяет выявить все возможные взаимодействия метрик и определить наиболее значимые из них. При построении системы защиты информации в облачных вычислениях определение значимых взаимодействий метрик инстансов является одним из ключевых факторов эффективной защиты. Моделирование информационной системы посредствам формирования матрицы смежности позволит использовать ее математические свойства, для определения поведения злоумышленника при реализации той или иной угрозы информационной безопасности.

Матрица смежности состоит из N строк и N столбцов, где N представляет из себя кортеж из вершин графа (3):

$$N = (R, R_1, R_2, R_3, R_4, R_5, R_6, C, C_1, S, S_1, S_2, S_3, S_4, S_5, N, N_2, N_3, N_4) \quad (3)$$

В таком случае матрица смежности M для графа состояния SYS примет вид (4):

$$M(SYS) = \begin{matrix} 01000001010000000000 \\ 10100000000000000000 \\ 01010000000000000000 \\ 00101000000000000000 \\ 00010100000000000000 \\ 00001010000000001000 \\ 00000100100000000000 \\ 10000000100000000000 \\ 00000011000000010000 \\ 10000000001000010000 \\ 00000000010100000000 \\ 00000000001010000000 \\ 00000000000101000000 \\ 00000000000010100000 \\ 00000000000001000000 \\ 00000100110000001000 \\ 00000000000000010000 \\ 00000000000000001010 \\ 00000000000000000101 \\ 00000001000000000010 \end{matrix} \quad (4)$$

Значение 1 на пересечении элементов матрицы означает что вершины графа, соответствующие данным элементам смежны, т.е. соответствующие метрики взаимодействуют между собой. Значение 0 означает что вершины не смежны, и метрики, соответствующие данным вершинам, не находятся во взаимодействии.

Примером практического использования данного взаимодействия может служить детектирование атаки типа «отказ в обслуживании» или DDoS атаки, характерными особенностями которой являются резкое изменение сетевой активности, выраженное в увеличении объема входящего трафика значительное повышение объемов затрачиваемой оперативной памяти и повышение времени загрузки процессора. Пример изменения метрик при DDoS атаке представлен на рисунке 3.

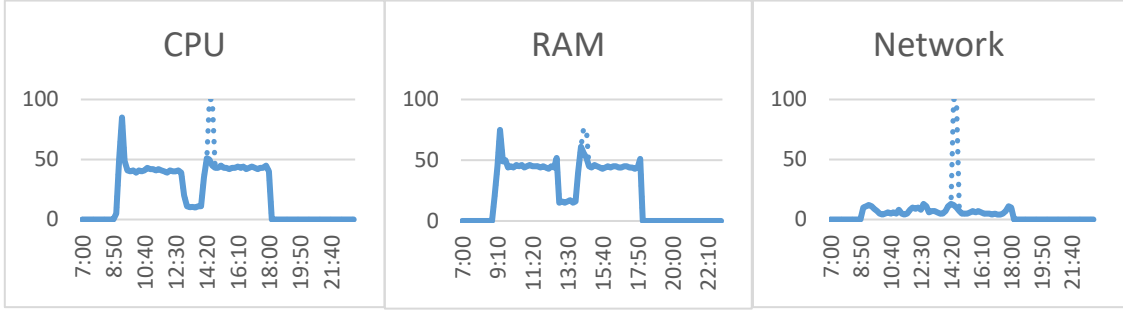

Рис.3. Изменение метрик системы при DDoS атаке.

Также с помощью описания взаимодействий различных параметров можно определить различные типы вирусных атак. К примеру, при атаке вируса майнера наблюдается резкий скачек параметра загрузки центрального процессора, значительное увеличение объемов затрачиваемой оперативной памяти и повышение сетевой активности. Пример изменения вышеупомянутых метрик представлен на рисунке 4.

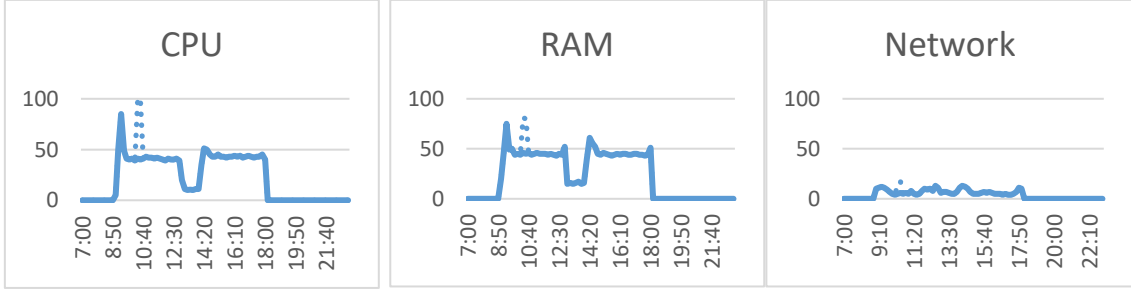

Рис.4. Изменение метрик системы при атаке вируса майнера.

Выявив все проблемные характеристики, система принятия решений направляет обращение к базе знаний, которая содержит описания существующих угроз и методы их устранения.

Сравнив информацию из базы знаний с текущими оценочными коэффициентами, система принятия решений формирует список возможных угроз, которые реализуются в данный момент. Основываясь на данном списке могут быть приняты меры для устранения всех угроз, которые в максимальной степени соответствуют описанию и отмечены значением «1».

Успешно приняв меры по устранению угроз, система принятия решений присылает уведомление системному администратору о проведённых действиях и текущем состоянии системы, а также предоставляет варианты стабилизации работы информационной системы, при необходимости.

При столкновении с угрозой, которой нет в базе данных, или которая не позволяет однозначно идентифицировать ситуацию, устройства автоматически отключаются от общей сети, помимо этого отправляется уведомление о неизвестной угрозе с описанием параметров системы в текущий момент.

Заключение

Модификация методики определения угроз информационной безопасности инстансов облачной инфраструктуры, основанной на теории графов, по средствам описания взаимодействия различных параметров системы между собой способствует повышению эффективности определения типов угроз, реализуемых злоумышленником. Применение данного подхода способствует оперативному реагированию на реализацию известных угроз информационной безопасности облачной инфраструктуры, а также может позволить сформировать представление о неизвестном типе угрозы.

Литература

1. *Темченко В. И., Цветков А. Ю.* Проектирование модели информационной безопасности в операционной системе //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). 2019. С. 740-745.

2 *Красов А.В., Штеренберг С.И., Голузина Д.Р* Методика визуализвции больших данных в системах защиты информации для формирования отчетов уязвимостей //Электросвязь. 2019. № 11. С. 39-47.

3. *Волкогонов В. Н., Гельфанд А. М., Деревянко В. С*. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). 2019. С. 262-266.

4. *Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А*., Защита для распределенных отказов в обслуживании в облачных вычислениях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). 2019. С. 329-334.

5. *Андрианов В.И., Виткова Л.А., Сахаров Д.В.* Исследование алгоритма защиты общедоступных персональных данных в информационных системах В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 227-231.

6. *Красов А.В., Штеренберг С.И., Москальчук А.И.* Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Брянского государственного технического университета. 2020. № 3 (88). С. 38-46.

7. *Штеренберг С.И., Москальчук А.И., Красов А.В*. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения //Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 47-58.

8. *Красов А.В., Левин М.В., Фостач Е.С*. Проблемы обеспечения безопасности облачных вычислений // В книге: Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. 2017. С. 520-522

9. *Миняев А.А., Красов А.В*. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 26-32.

10. *Красов А.В., Сахаров Д.В., Тасюк А.А*. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 1. С. 70-76.

11. *Красов А.В., Штеренберг С.И., Голузина Д.Р*. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. № 11. С. 39-47.

12. *Виткова Л.А., Иванов А.И., Сергеева И.Ю.* Исследование и разработка методик оценки рисков облачных ресурсов // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 152-155

13. *Виткова Л.А., Глущенко А.А., Сахаров Д.В., Чмутов М.В*. Выбор оптимального метода оценки эффективности перехода к облачной архитектуре. // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 168-171.

14. *Виткова Л.А., Иванов А.И*. Обзор актуальных угроз и методов защиты в сфере облачных вычислений. //В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 179-182.

DESCRIPTION OF THE INTERACTIONS OF VARIOUS SYSTEM METRICS WHEN USING A TECHNIQUE FOR IDENTIFYING THREATS TO THE INFORMATION SECURITY OF CLOUD INFRASTRUCTURE INSTANCES BASED ON GRAPH THEORY

IGOR E. PESTOV,
St-Petersburg, Russia, ip@sut.ru

PAVEL O. FEDOROV,
St-Petersburg, Russia, pavel_lenin@mail.ru

EKATERINA S. FEDOROVA,
St-Petersburg, Russia, ek.chukina@yandex.ru

ILYA A. SMUROV,
St-Petersburg, Russia, ismurov@mail.ru

ABSTRACT

Introduction: This paper deals with the problem of information security of cloud infrastructure instances. **Purpose:** In this work, it is necessary to describe the interactions of various system metrics when using a methodology for identifying threats to the information security of cloud infrastructure instances based on graph theory. **Results:** The description of the interactions of various system parameters is given, which is used to construct a system state graph. The description of these interactions contributes to a more detailed analysis of the state of the system when various threats to information security are implemented by an attacker. The article provides specific examples of changes in cloud infrastructure metrics that are typical for such types of threats as a denial of service attack and a miner virus attack. **Practical relevance**: This method allows to increase the efficiency of identifying threats to the information security of cloud infrastructure instances. **Discussion:** As further research, a detailed consideration of anomalies in the interaction of various cloud infrastructure metrics characteristic of unknown types of threats is required.

Keywords: cloud infrastructure; information security; metric; instance; virtual machine; container.

REFERENCES

1. Temchenko V.I., Tsvetkov A.Y. Designing an information security model in the operating system. Actual problems of infotelecommunications in science and education (APINO 2019). 2019. Pp. 740-745.
2. Krasov A.V., Shterenberg S.I., Goluzina D.R. Big data visualization technique in information security systems for vulnerability reporting. Telecommunications. 2019. No. 11. Pp. 39-47.
3. Volkogonov V. N., Gelfand A. M., Derevyanko V. S. Relevance of automated control systems. Actual problems of infotelecommunications in science and education (APINO 2019). 2019. Pp. 262-266.
4. Gelfand A. M., Kosov N. A., Krasov A. V., Orlov G. A., Protection for distributed denial of service in cloud computing. Actual problems of infotelecommunications in science and education (APINO 2019). 2019. Pp. 329-334.
5. Andrianov V.I., Vitkova L.A., Sakharov D.V. Study of the algorithm for protecting publicly available personal data in information systems In the collection: Actual problems of info-telecommunications in science and education. Collection of scientific articles of the V international scientific-technical and scientific-methodical conference. 2016. Pp. 227-231.
6. Krasov A.V., Shterenberg S.I., Moskalchuk A.I. Methodology for creating a virtual laboratory for testing the security of distributed information systems. Bulletin of the Bryansk State Technical University. 2020. No. 3 (88). Pp. 38-46.
7. Shterenberg S.I., Moskalchuk A.I., Krasov A.V. Development of security scenarios for the creation of vulnerable virtual machines and the study of penetration testing methods.Information technologies and telecommunications. 2021. Vol. 9. No. 1. Pp. 47-58.
8. Krasov A.V., Levin M.V., Fostach E.S. Problems of ensuring the security of cloud computing. In the book: Information Security of Russian Regions (ISRR-2017). Conference materials. 2017. Pp. 520-522.
9. Minyaev A.A., Krasov A.V. Methodology for evaluating the effectiveness of the information protection system of geographically distributed information systems. Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and technical sciences. 2020. No. 3. Pp. 26-32.
10. Krasov A.V., Sakharov D.V., Tasyuk A.A. Designing an intrusion detection system for an information network using big data. Science-intensive technologies in space research of the Earth. 2020. Vol. 12. No. 1. Pp. 70-76.
11. Krasov A.V., Shterenberg S.I., Goluzina D.R. Big Data Visualization Technique in Information Security Systems for Vulnerability Reporting. Elektrosvyaz. 2019. No. 11. Pp. 39-47.
12. Vitkova L.A., Ivanov A.I., Sergeeva I.Yu. Research and development of methods for assessing the risks of cloud resources. In the collection: Actual problems of infotelecommunications in science and education (APINO 2017). Collection of scientific articles of the VI International scientific- technical and scientific-methodical conference. In 4 volumes. Edited by S.V. Bachevsky. 2017. Pp. 152-155.
13. Vitkova L.A., Glushchenko A.A., Sakharov D.V., Chmutov M.V. Choosing the optimal method for evaluating the effectiveness of the transition to cloud architecture. In the collection: Actual problems of infotelecommunications in science and education (APINO 2018). VII International scientific-technical and scientific-methodical conference. Collection of scientific articles. In 4 volumes. Edited by S.V. Bachevsky. 2018. Pp. 168-171.
14. Vitkova L.A., Ivanov A.I. Overview of current threats and protection methods in the field of cloud computing. In the collection: Actual problems of infotelecommunications in science and education (APINO 2018). VII International scientific-technical and scientific-methodical conference. Collection of scientific articles. In 4 volumes. Edited by S.V. Bachevsky. 2018. Pp. 179-182.