Russian Technological Journal. 2022;10(1):28–34

ISSN 2500-316X (Online)

UDC 519.7
https://doi.org/10.32362/2500-316X-2022-10-1-28-34

RESEARCH ARTICLE

Data backup methods for mission-critical information systems

Sergey V. Shaytura [1, 2, @], Pavel N. Pitkevich [3]

[1] *Institute of Humanities, Economics and Information Technologies, Burgas, 8000 Bulgaria*
[2] *Russian University of Transport, Moscow, 127055 Russia*
[3] *Belarusian State University of Informatics and Radioelectronics, Minsk, 220013 Belarus*
[@] *Corresponding author, e-mail: swshaytura@gmail.com*

Abstract

Objectives. Digitalization of the economy has led to a situation in which organizations accumulate huge amounts of digital data, the loss or damage of which leads to irreparable damage to the organizations. The issue of increasing data safety is relevant. One of the ways to improve the safety of data is backing them up. The study aimed to develop an effective strategy for backing up data for critical enterprise information systems.

Methods. The method for solving the problem was to create backup copies of enterprise information systems using a flexible architecture based on the backup—as a service in external cloud structures—in combination with technical resources of the organization.

Results. This article discussed backup solutions and tools, which include: backup volumes and schedule, target point and recovery time. The strategies and mechanisms of data backup were analyzed. The most common backup mechanisms are removable media, backups, external hard drive, hardware, backup software, cloud backup services. To create backups on a network, a large external hard drive is created and archival software is used to save changes to local files on that hard drive. This article covered: backup strategy, concept of backup storage, different types of backup storage methods, including network storage, external hard drives, and cloud storage. The main provisions and rules for backing up critical information systems were described. The rules for copying servers were given.

Conclusions. This article discusses a data backup architecture for mission-critical enterprise information systems. The authors believe that there should be at least three backups, two of which are located in the “cloud.” The 3–2–1 strategy developed by the authors gives quite satisfactory results for the safety of critical data.

Keywords: backup, data recovery, network storage, cloud technologies, banking sector, hybrid clouds

• **Submitted:** 13.09.2021 • **Revised:** 14.10.2021 • **Accepted:** 15.12.2021

For citation: Shaytura S.V., Pitkevich P.N. Data backup methods for mission-critical information systems. *Russ. Technol. J.* 2022;10(1):28–34. https://doi.org/10.32362/2500-316X-2022-10-1-28-34

Financial disclosure: The authors have no a financial or property interest in any material or method mentioned.

The authors declare no conflicts of interest.

НАУЧНАЯ СТАТЬЯ

Методы резервирования данных для критически важных информационных систем предприятия

С.В. Шайтура [1, 2, @], П.Н. Питкевич [3]

[1] *Институт гуманитарных наук, экономики и информационных технологий, Бургас, 8000 Болгария*
[2] *Российский университет транспорта, Москва, 127055 Россия*
[3] *Белорусский государственный университет информатики и радиоэлектроники, Минск, 220013 Беларусь*
[@] *Автор для переписки, e-mail: swshaytura@gmail.com*

Резюме

Цели. Цифровизация экономики привела к тому, что любая организация накапливает огромное количество цифровых данных, потеря или порча которых приводит к невосполнимому ущербу для организации. Актуальным является вопрос повышения сохранности данных. Одним из способов повышения сохранности данных является резервное копирование. Целью статьи является разработка эффективной стратегии резервирования данных для критически важных информационных систем предприятия.

Методы. Методом решения задачи является создание резервных копий информационных систем предприятия на основе применения гибкой архитектуры, основанной на сочетании резервного копирования как услуги во внешних облачных структурах с техническими средствами, находящимися в распоряжении организации.

Результаты. В статье обсуждаются решения и инструменты для резервного копирования, среди которых: объемы и расписание резервного копирования, целевая точка и время восстановления данных. Рассмотрены стратегии и механизмы резервного копирования данных. Наиболее распространенными механизмами резервного копирования являются съемные носители, резервирование, внешний жесткий диск, аппаратные средства, программное обеспечение для резервного копирования, услуги резервного копирования в «облако». Для создания резервных копий в своей сети создается внешний жесткий диск большого объема и используется архивное программное обеспечение для сохранения изменений в локальных файлах на этом жестком диске. В статье рассмотрены: стратегия резервного копирования, концепция хранилища резервных копий, различные типы методов хранения резервных копий, включая сетевое хранилище, внешние жесткие диски и облачное хранилище. Описаны основные положения и правила резервного копирования критически важных информационных систем. Приведены правила копирования серверов.

Выводы. В статье обсуждается архитектура резервного копирования данных для критически важных информационных систем предприятия. Авторы считают, что резервных копий должно быть не менее трех, две из которых размещаются в «облаке». Разработанная авторами стратегия 3–2–1 дает вполне удовлетворительные результаты по сохранности критически важных данных.

Ключевые слова: резервное копирование, восстановление данных, сетевое хранилище, облачные технологии, банковский сектор, гибридные «облака»

• **Поступила:** 13.09.2021 • **Доработана:** 14.10.2021 • **Принята к опубликованию:** 15.12.2021

Для цитирования: Шайтура С.В., Питкевич П.Н. Методы резервирования данных для критически важных информационных систем предприятия. *Russ. Technol. J.* 2022;10(1):28–34. https://doi.org/10.32362/2500-316X-2022-10-1-28-34

Прозрачность финансовой деятельности: Никто из авторов не имеет финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

INTRODUCTION

In the digital economy [1], backing up data [2–4] is vital for the functioning of an organization [5]. Data can be stolen, corrupted, or lost. Data backup is a practice that combines methods and solutions for efficient and economical data storage with the process of parallel computing [6, 7], that leads to a synergistic effect [8, 9]. Corporate data are copied to one or more locations at predetermined frequency and varying capacities. A flexible backup operation can be set up using either the company's own architecture or the available Backup as a Service (BaaS) solutions, mixing them with local storage [10–12]. Today there are many technical solutions for corporate storage [13], which allow the company to protect data [14–16], avoid their loss, prevent leakage, and calculate costs [17–19].

Data backup is the practice of copying information from a primary to a secondary location to protect it in the event of a disaster, accident, or malicious act. Data is a vital resource of modern organizations, and its loss can cause serious damage to security [20, 21]. Therefore, backups are critical for all businesses.

The most common causes of data loss are hardware and system failure (31%), human error (29%), viruses and ransomware (29%) [14, 22, 23].

METHODS FOR SOLVING THE PROBLEM

Typically, backup data is essential information for workloads running on a corporate server. These can include documents, media files, configuration files, computer images, operating systems, and registry files. Basically, any data that needs to be saved can be backed up.

Backing up data includes several important concepts.

Backup solutions and tools. While it is possible to manually back up the data, in order to ensure that this is done regularly and consistently, most organizations use technology-based solutions to back up their data.

Backup administrator. Each organization should designate a backup administrator. This person verifies that the backup systems are configured correctly, tests them periodically, and ensures that critical data is actually backed up.

The volume and schedule of backups. An organization should choose a backup policy, specifying which files and systems are important enough to back up and how often to back it up.

Recovery Point Objective (*RPO*). This is the amount of data that an organization is prepared to lose in the event of a disaster, and it is determined by the frequency of backups. If the systems are backed up once a day, the RPO is 24 h. The lower the RPO, the more storage, compute, and network resources are required for frequent backups.

Recovery Time Objective (*RTO*). This is the time it takes for an organization to restore data or systems from a backup and resume normal operation. For large amounts of data and/or backups stored off-site, copying data and restoring systems can take a significant amount of time. Reliable technical solutions are required to ensure low RTO values.

DATA BACKUP MECHANISMS

There are many ways to back up a file [3, 24, 25]. Choosing the right option can help an organization to create the best backup plan. The most common backup mechanisms are: removable media, backups, external hard drive, hardware, backup software, cloud backup services.

An easy option is to back up the files to removable media such as CDs, DVDs, Blu-Ray discs, or USB drives.

An additional hard drive can be configured, which will be a copy of the drive of critical information systems of the enterprise. It is possible set up a large external hard drive on your network and use archive software to save changes to local files on that hard drive. The archiving software allows you to recover files from external hardware in just a few minutes. However, as data volumes grow, a single external drive will not be enough.

Many vendors provide off-the-shelf backup devices, typically 19″ rack mountable. Backup devices come with large storage capacities and pre-integrated software. Backup agents are installed on the systems for which you want to run the backup, a schedule and backup policy are defined, and data are transferred to the backup device. As with the other options, you can place the backup device isolated from the local network and, if possible, in a remote location.

Backup software solutions are more difficult to set up and configure than hardware appliances, but they provide more flexibility. They allow you to determine which systems and data will be backed up, place the backups on the selected storage device, and automatically manage this process.

Cloud providers offer BaaS solutions where you can send on-premises data to the public or private cloud, and in the event of a disaster, recover the data back from the cloud. BaaS solutions are easy to use; their great advantage is that the data are stored remotely. However, when using the public cloud, you must comply with applicable regulations and standards, and bear in mind that over time, the cost of storing data in the cloud will be much higher than the cost of setting up similar storage locally.

STRATEGY 3–2–1 BACKUP FOR CRITICAL CORPORATE INFORMATION SYSTEMS

The authors proposed a 3–2–1 backup strategy for critical corporate information systems. This strategy is to ensure that systems are adequately backed up and recovered reliably. The essence of the strategy is that three copies of important information systems of an organization are created on at least two different media, and at least one copy is stored remotely.

Three copies of the data include the original data and two duplicates. This ensures that a lost backup or damaged media will not affect your ability to recover.

Two different storage types reduce the risk of media-specific failures by using two different technologies. Common options include internal and external hard drives, removable media, or cloud storage

In this case, one copy is stored directly in the organization. Incremental or differential backups are performed daily. There are two backups in different remote locations ("cloud"). Once a week, a full copy of the computer disks is made and sent to "cloud" No. 1. Additionally, once a month, another full copy is made, the results of which are sent to "cloud" No. 2. The composition of the daily and weekly set is constant. Thus, compared to simple rotation, the archive contains only monthly copies and the latest weekly and daily copies.

One remote copy eliminates the risk of a single point of failure. External copies are essential for robust disaster recovery and data backup strategies, and can provide failover during local failures when needed.

BACKUP OF CRITICAL IT SYSTEMS

The easiest way to back up a server is the solutions proposed in [10, 11]. This is a full server backup. It can be performed weekly, monthly, or quarterly and performed using compression techniques. These solutions are usually designed to help back up server data to another on-premises server, cloud server, or hybrid system. In particular, backups to hybrid systems are becoming increasingly popular. This is because such systems can optimize resources, support simple redundancy across multiple regions, and can provide faster recovery and failover.

Typically, server backup solutions should include the following functions.

Support for various file types. All kinds of files must be supported. In particular, solutions must support documents, spreadsheets, media files, and configuration files.

Backup location. It should be possible to specify the backup locations. The solution should support backups to multiple locations and media, including internal and external resources.

Scheduling and automation. In addition to be able to perform manual backups, solutions must support the automation of backups through scheduling. This ensures that the user always has the most recent backup and that the backups are created in a consistent manner.

Backup management. You need to be able to manage the lifecycle of your backups, including the number and length of storage. Ideally, solutions also make it easy to export backups for transfer to external resources.

Section selection. Partitions are isolated segments of a storage resource and are often used to separate data on a system. Solutions should allow users to self-back up and recover partitions.

Compression of data. To minimize the amount of storage required for multiple backups, solutions must compress the backup data. This compression must be lossless and maintain the integrity of all data.

Selecting the type of backup. It should be possible to create various types of backups, including full, differential and incremental. Differential backups contain a copy of the changes since the last full backup, while incremental backups contain a record of the changes since the last incremental backup. This can help reduce the size of backups and speed up backup times.

Scaling. Backup capabilities should not be limited by the amount of data on users' servers. Solutions must be scaled as well as data and support backups of any size.

BACKUP TECHNOLOGY

Backup storage is the physical location or device for storing copies of data for recovery in the event of a disaster or data loss. Backup storage systems typically include both hardware and software for backup and recovery management. This includes everything from simple flash storage to hybrid local physical storage and remote cloud storage.

Whichever method is used for backup, in the end, the data must be stored somewhere [12–14]. The technology used to store the backup data is very important. The more economical the technology, the more data can be stored and the faster that data will be retrieved. The more reliable the storage technology, the more reliable will be the safety of backups.

Network resources and NAS. You can configure centralized storage such as Network Attached Storage (NAS), Storage Area Network (SAN), or regular hard drives connected as a network share using the Network File System (NFS) protocol. This is a convenient option for providing local devices with a large amount of backup storage. However, it is susceptible to threats such as fire, flooding and other threats of destruction affecting the entire data center, as well as cyber attacks.

Cloud storage of objects. When using cloud providers, there is access to a variety of storage services. There are tools that allow you to automatically create backups of data, both from the "cloud" and from local machines. The most popular are:

AMANDA (Advanced Maryland Automatic Network Disk Archiver) is a system for backing up and archiving information.

Bacula is a client/server software that allows you to manage backup, recover and validate data over the network for computers and operating systems of various types.

Duplicity is backs up encrypted volumes in tar-format locally or to a remote host.

CONCLUSIONS

This article discusses a data backup architecture for mission-critical enterprise information systems. The authors believe that there should be at least three backups, two of which are located in the "cloud." The 3–2–1 strategy developed by the authors gives quite satisfactory results for the safety of critical data. It protects against both accidents and malicious threats such as ransomware and provides reliable data backup and recovery.

Authors' contribution. All authors equally contributed to the research work.

REFERENCES

1. Tsvetkov V.Ya., Shaytura S.V., Sultaeva N.L. Digital enterprise management in cyberspace. In: *Advances in Economics, Business and Management Research*. Proceedings of the 2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020). 2020. P. 361–365. https://dx.doi.org/10.2991/aebmr.k.200502.059
2. Santos D., Gomes T. Joint optimization of primary and backup controller placement and availability link upgrade in SDN networks. *Optical Switching and Networking*. 2021;42:100634. https://doi.org/10.1016/j.osn.2021.100634
3. Jin D., Wang Q. CDP backup and recovery method for ensuring database consistency. In: *2021 IEEE International Conference on Power Electronics, Computer Applications* (*ICPECA*). 2021. P. 722–728. https://doi.org/10.1109/ICPECA51329.2021.9362541
4. Mao J., Chen L., Li J., Ge Y. Controller backup and replication for reliable multi-domain SDN. *KSII T Internet Info*. 2020;14(12):4725−4747. https://doi.org/10.3837/tiis.2020.12.006
5. Kulagin V. Global or world security? *Mezhdunarodnye protsessy = International Trends*. 2007;5(2–14):38−51 (in Russ.).
6. Kulagin V.P. Problems of parallel computing systems. *Perspektivy nauki i obrazovaniya = Perspectives of Science and Education*. 2016;1(19):7−11 (in Russ.).
7. Kulagin V.P. Problems of analysis and synthesis of structures of parallel computing systems. *Vestnik MGTU MIREA*. 2013;1:1−19 (in Russ.).
8. Ivannikov A.D., Kulagin V.P., Mironov A.A., Mordvinov V.A., Sigov A.S., Tikhonov A.N., Tsvetkov V.Ya. *Sinergeticheskaya teoriya informatsionnykh protsessov i sistem* (*Synergetic theory of information processes and systems*). Moscow: MIREA; 2010. 455 p. (in Russ.). ISBN 978-5-7339-0841-0
9. Khandare L., Sreekantha D.K. Analysis on privacy protection in cloudlet and edge technology. In: *2019 5th International Conference on Computing, Communication, Control and Automation* (*ICCUBEA*). 2019. 5 p. https://doi.org/10.1109/ICCUBEA47591.2019.9128645

СПИСОК ЛИТЕРАТУРЫ

1. Tsvetkov V.Ya., Shaytura S.V., Sultaeva N.L. Digital enterprise management in cyberspace. In: *Advances in Economics, Business and Management Research*. Proceedings of the 2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020). 2020. P. 361−365. https://dx.doi.org/10.2991/aebmr.k.200502.059
2. Santos D., Gomes T. Joint optimization of primary and backup controller placement and availability link upgrade in SDN networks. *Optical Switching and Networking*. 2021;42:100634. https://doi.org/10.1016/j.osn.2021.100634
3. Jin D., Wang Q. CDP Backup and Recovery Method for Ensuring Database Consistency. In: *2021 IEEE International Conference on Power Electronics, Computer Applications* (*ICPECA*). 2021. P. 722−728. https://doi.org/10.1109/ICPECA51329.2021.9362541
4. Mao J., Chen L., Li J., Ge Y. Controller backup and replication for reliable multi-domain SDN. *KSII T Internet Info*. 2020;14(12):4725−4747. https://doi.org/10.3837/tiis.2020.12.006
5. Кулагин В. Глобальная или мировая безопасность? *Международные процессы*. 2007;5(2–14):38−51.
6. Кулагин В.П. Проблемы параллельных вычислений. *Перспективы науки и образования*. 2016;1(19):7−11.
7. Кулагин В.П. Проблемы анализа и синтеза структур параллельных вычислительных систем. *Вестник МГТУ МИРЭА*. 2013;1:1−19.
8. Иванников А.Д., Кулагин В.П., Миронов А.А., Мордвинов В.А., Сигов А.С., Тихонов А.Н., Цветков В.Я. *Синергетическая теория информационных процессов и систем*. М.: МИРЭА; 2010. 455 с. ISBN 978-5-7339-0841-0
9. Khandare L., Sreekantha D.K. Analysis on privacy protection in cloudlet and edge technology. In: *2019 5th International Conference on Computing, Communication, Control and Automation* (*ICCUBEA*). 2019. 5 p. https://doi.org/10.1109/ICCUBEA47591.2019.9128645

10. Chitra S., Madhusudhanan B., Sakthidharan G.R., Saravanan P. Local minima jump PSO for workflow scheduling in cloud computing environments. In: Jeong H., S. Obaidat M., Yen N., Park J. (Eds.). *Advances in Computer Science and its Applications*. *Lecture Notes in Electrical Engineering*. Berlin, Heidelberg: Springer. 2014. Vol. 279. P. 1225−1234. https://doi.org/10.1007/978-3-642-41674-3_170
11. Almutairi B. Secure mitigation and migration of virtual machines over hybrid cloud hypervisors infrastructure. *International Journal of Advanced and Applied Sciences*. 2021;8(7):7−13. https://doi.org/10.21833/ijaas.2021.07.002
12. Uskov A.V., Ivannikov A.D., Uskov V.L. Technologies for ensuring information security of corporate educational networks. *Obrazovatel'nye tekhnologii i obshchestvo = Educational Technologies & Society*. 2008;11(1):472−479 (in Russ.).
13. Bulgakov S.V., Koval'chuk A.K., Tsvetkov V.Ya., Shaitura S.V. *Zashchita informatsii v GIS* (*Information protection in GIS*). Moscow: MGTU im. Baumana; 2007. 183 p. (in Russ.).
14. Protasova A.A., Shaitura S.V. Analysis methods of data protection database. *Slavyanskii forum = Slavic Forum*. 2017;1(15):290−298 (in Russ.).
15. Dolmatov V.V., Gusev A.V., Grusho I.N., Kulagin V.P., Kuznetsov Yu.M. The use of personal information security devices in education. *Informatizatsiya obrazovaniya i nauki = Informatization of Education and Science*. 2009;2:38−45 (in Russ.).
16. Shaitura S.V., Feoktistova F.M., Minitaeva A.M., Olenev L.A., Chulkov V.O., Kozhaev Y.P. Spatial geomarketing powered by Big Data. *Revista Turismo: Estudos & Práticas*. 2020;S5:13.
17. Shaitura S.V., Ordov K.V., Lesnichaya I.G., Romanova Yu.D., Khachaturova S.S. Services and mechanisms of competitive intelligence on the internet. *Espacios*. 2018;39(45):24.
18. Zabotnev M.S., Kulagin V.P. Issues of access to information in incomplete databases. *Trudy mezhdunarodnogo simpoziuma "Nadezhnost' i kachestvo" = Proceedings of the International Symposium "Reliability and Quality."* 2005;1:195−196 (in Russ.).
19. Ivannikov A.D., Kulagin V.P., Tikhonov A.N., Tsvetkov V.Ya. *Informatsionnaya bezopasnost' v geoinformatike* (*Information security in geoinformatics*). Moscow: Maks Press; 2004. 334 p. (in Russ.). ISBN 5-317-00869-7
20. Golkina G.E., Shaitura S.V. *Bezopasnost' bukhgalterskikh informatsionnykh system* (*Security of Accounting Information Systems*). Burgas, Bulgaria: Institute of Humanities, Economics and Information Technology; 2016. 100 p. (in Russ.).
21. Kulagin V.P., Kuznetsov Yu.M., Zabotnev M.S. Methods and means of access of users of an open information learning environment to federal Internet resources. *Distantsionnoe i virtual'noe obuchenie = Distance & Virtual Education*. 2008;9:11−15 (in Russ.).
22. Ivannikov A.D., Kulagin V.P., Tikhonov A.N., Tsvetkov V.Ya. Digital steganography: enciphering, protection. *Informatsionnye tekhnologii = Information Technologies*. 2004;8:1−32. (Appendix to the journal) (in Russ.).

10. Chitra S., Madhusudhanan B., Sakthidharan G.R., Saravanan P. Local minima jump PSO for workflow scheduling in cloud computing environments. In: Jeong H., S. Obaidat M., Yen N., Park J. (Eds.). *Advances in Computer Science and its Applications*. *Lecture Notes in Electrical Engineering*. Berlin, Heidelberg: Springer. 2014. Vol. 279. P. 1225−1234. https://doi.org/10.1007/978-3-642-41674-3_170
11. Almutairi B. Secure mitigation and migration of virtual machines over hybrid cloud hypervisors infrastructure. *International Journal of Advanced and Applied Sciences*. 2021;8(7):7−13. https://doi.org/10.21833/ijaas.2021.07.002

12. Усков А.В., Иванников А.Д., Усков В.Л. Технологии обеспечения информационной безопасности корпоративных образовательных сетей. *Образовательные технологии и общество*. 2008;11(1):472−479.
13. Булгаков С.В., Ковальчук А.К., Цветков В.Я., Шайтура С.В. *Защита информации в ГИС*. М.: МГТУ им. Баумана; 2007. 187 с.
14. Протасова А.А., Шайтура С.В. Анализ методов защиты баз данных. *Славянский форум*. 2017;1(15):290−298.
15. Долматов В.В., Гусев А.В., Грушо И.Н., Кулагин В.П., Кузнецов Ю.М. Использование персональных устройств защиты информации в сфере образования. *Информатизация образования и науки*. 2009;2:38−45.
16. Shaitura S.V., Feoktistova F.M., Minitaeva A.M., Olenev L.A., Chulkov V.O., Kozhaev Y.P. Spatial geomarketing powered by Big Data. *Revista Turismo: Estudos & Práticas*. 2020;S5:13.
17. Shaitura S.V., Ordov K.V., Lesnichaya I.G., Romanova Yu.D., Khachaturova S.S. Services and mechanisms of competitive intelligence on the internet. *Espacios*. 2018;39(45):24.
18. Заботнев М.С., Кулагин В.П. Вопросы доступа к информации в неполных базах данных. *Труды международного симпозиума «Надежность и качество»*. 2005;1:195−196.
19. Иванников А.Д., Кулагин В.П., Тихонов А.Н., Цветков В.Я. *Информационная безопасность в геоинформатике*. М.: Макс Пресс; 2004. 334 с. ISBN 5-317-00869-7
20. Голкина Г.Е., Шайтура С.В. *Безопасность бухгалтерских информационных систем*. Бургас: Институт гуманитарных наук, экономики и информационных наук; 2016. 100 с.
21. Кулагин В.П., Кузнецов Ю.М., Заботнев М.С. Методы и средства доступа пользователей открытой информационной среды обучения к федеральным Интернет-ресурсам. *Дистанционное и виртуальное обучение*. 2008;9:11−15.
22. Иванников А.Д., Кулагин В.П., Тихонов А.Н., Цветков В.Я. Цифровая стеганография: шифрование, защита. *Информационные технологии*. 2004;8:1−32. (Приложение к журналу).
23. Faria H., Hagstrom R., Reis M., Costa B.G.S., Ribeiro E., Holanda M., Barreto P.S., Araújo A. A Hadoop open source backup solution. In: *Proceedings of the 8th International Conference on Cloud Computing and Services Science* (*CLOSER*). 2018. P. 651−657. https://doi.org/10.5220/0006809206510657

23. Faria H., Hagstrom R., Reis M., Costa B.G.S., Ribeiro E., Holanda M., Barreto P.S., Araújo A. A Hadoop open source backup solution. In: *Proceedings of the 8th International Conference on Cloud Computing and Services Science* (*CLOSER*). 2018. P. 651–657. https://doi.org/10.5220/0006809206510657
24. Ivannikov A.D., Levchenko N.N., Okunev A.S., Stempkovsky A.L., Zmejev D.N. Dataflow computing model – perspectives, advantages and implementation. In: *Proceedings of 2017 IEEE East-West Design & Test Symposium* (*EWDTS*). 2017. P. 8110117. https://doi.org/10.1109/EWDTS.2017.8110117
25. Tikhonov A.N., Ivannikov A.D., Solov'ev I.V., Tsvetkov V.Ya., Kudzh S.A. *Kontseptsiya setetsentricheskogo upravleniya slozhnoi organizatsionno-tekhnicheskoi sistemoi* (*The concept of network-centric management of a complex organizational and technical system*). Moscow: MAKS Press; 2010. 136 p. (in Russ.). ISBN 978-5-317-03246-3

24. Ivannikov A.D., Levchenko N.N., Okunev A.S., Stempkovsky A.L., Zmejev D.N. Dataflow computing model – perspectives, advantages and implementation. In: *Proceedings of 2017 IEEE East-West Design & Test Symposium* (*EWDTS*). 2017. P. 8110117. https://doi.org/10.1109/EWDTS.2017.8110117
25. Тихонов А.Н., Иванников А.Д., Соловьев И.В., Цветков В.Я., Кудж С.А. *Концепция сетецентрического управления сложной организационно-технической системой*. М.: МАКС Пресс; 2010. 136 с. ISBN 978-5-317-03246-3

About the authors

Sergey V. Shaytura, Associate Professor, Russian University of Transport (9/9, Obraztsova ul., Moscow, 127055 Russia); Rector of the Institute of Humanities, Economics and Information Technologies (88, Angela Dimitrova ul., Burgas, 8000 Bulgaria). E-mail: swshaytura@gmail.com. Scopus Author ID 57190974935, ResearcherID D-9102-2016, https://orcid.org/0000-0002-5621-5460

Pavel I. Pitkevich, Postgraduate Student, Belarusian State University of Informatics and Radioelectronics (6, P. Brovki ul., Minsk, 220013 Republic of Belarus). E-mail: pavel.pitkevich@gmail.com.

Об авторах

Шайтура Сергей Владимирович, доцент, Российский университет транспорта (127055, Россия, Москва, ул. Образцова, д. 9, стр. 9); ректор Института гуманитарных наук, экономики и информационных технологий (8000, Болгария, Бургас, ул. Ангела Димитрова, д. 88). E-mail: swshaytura@gmail.com. Scopus Author ID 57190974935, ResearcherID D-9102-2016, https://orcid.org/0000-0002-5621-5460

Питкевич Павел Игоревич, аспирант, Белорусский государственный университет информатики и радиоэлектроники (220013, Республика Беларусь, Минск, ул. П. Бровки, д. 6). E-mail: pavel.pitkevich@gmail.com.

Translated by E. Shklovskii
The abstract was edited for English language and spelling by Q. Scribner, Awatera