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

ISSN 2782-3210 (Print)
ISSN 2500-316X (Online)

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

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.

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.

ВВЕДЕНИЕ

В условиях цифровой экономики [1] резервное копирование данных [2–4] жизненно важно для функционирования организации [5]. Данные могут быть украдены, испорчены или потеряны. Резервное копирование данных – это практика, сочетающая методы и решения эффективного и экономичного сохранения данных с процессом параллельных вычислений [6, 7], что приводит к появлению синергетического эффекта [8, 9]. Данные организации копируются в одном или нескольких местах с заранее определенной частотой и разной емкостью. Можно настроить гибкую операцию резервного копирования, используя собственную архитектуру, или использовать доступные решения «Резервное копирование как услуга» (англ. backup as a service, BaaS), смешивая их с локальным хранилищем [10–12]. Сегодня существует множество решений технических средств для корпоративных хранилищ [13], которые позволяют защитить данные [14–16], избежать их потери и предотвратить утечку, рассчитать затраты [17–19].

Резервное копирование данных – это практика копирования информации из основного во второстепенное место для их защиты в случае бедствия, аварии или злонамеренного действия. Данные – жизненно важный ресурс современных организаций, их потеря может нанести серьезный ущерб безопасности [20, 21]. Поэтому резервное копирование имеет решающее значение для всех предприятий.

Наиболее частыми причинами потери данных являются аппаратный/системный сбой (31%), человеческий фактор (29%), вирусы и вредоносные программы-вымогатели (29%) [14, 22, 23].

МЕТОДЫ РЕШЕНИЯ ЗАДАЧИ

Обычно данные резервного копирования – это необходимая информация для рабочих нагрузок, выполняемых сервером организации или предприятия. Это могут быть документы, мультимедийные файлы, файлы конфигурации, образы компьютеров, операционные системы и файлы реестра. По сути, любые данные, которые необходимо сохранить, можно сохранить как резервную копию.

Резервное копирование данных включает в себя несколько важных концепций.

Решения и инструменты для резервного копирования. Хотя можно создавать резервные копии данных вручную, чтобы обеспечить этот процесс регулярно и последовательно, большинство организаций используют технологические решения для резервного копирования своих данных.

Администратор резервного копирования. Каждая организация должна назначить сотрудника, ответственного за резервное копирование. Этот сотрудник проверяет, что системы резервного копирования настроены правильно, периодически тестирует их и обеспечивает фактическое резервное копирование критически важных данных.

Объем и расписание резервного копирования. Организация должна выбрать политику резервного копирования, указав, какие файлы и системы достаточно важны для копирования и как часто следует его выполнять.

Целевая точка восстановления (англ. recovery point objective, RPO). Это объем данных, который организация готова потерять в случае аварии, он определяется частотой резервного копирования. Если резервное копирование систем выполняется один раз в день, RPO составляет 24 часа. Чем ниже RPO, тем больше ресурсов хранения данных, вычислительных и сетевых ресурсов требуется для частого резервного копирования.

Целевое время восстановления (англ. recovery time objective, RTO). Это время, необходимое организации для восстановления данных или систем из резервной копии и возобновления нормальной работы. Для больших объемов данных и/или резервных копий, хранящихся за пределами предприятия, копирование данных и восстановление систем может занять значительное время. Для обеспечения небольших значений RTO необходимы надежные технические решения.

МЕХАНИЗМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ ДАННЫХ

Есть много способов сделать резервную копию файла [3, 24, 25]. Выбор правильного варианта может помочь создать оптимальный план резервного копирования данных для нужд организации. Наиболее распространенными механизмами резервного копирования являются: съемные носители, резервирование, внешний жесткий диск, аппаратные средства, программное обеспечение для резервного копирования, услуги резервного копирования в «облако».

Простым вариантом является резервное копирование файлов на съемные носители: CD, DVD, диски Blu-Ray или USB-накопители.

Можно настроить дополнительный жесткий диск, который будет являться копией диска важных информационных систем предприятия. Возможно развернуть в своей сети внешний жесткий диск большого объема и использовать архивное программное обеспечение для сохранения изменений в локальных файлах на этом жестком диске. Программное обеспечение для архивирования позволяет восстанавливать файлы с внешнего оборудования с резервного программного обеспечения всего за несколько минут.

Однако по мере роста объемов данных одного внешнего диска будет недостаточно.

Многие поставщики предоставляют готовые устройства резервного копирования, обычно устанавливаемые в 19-дюймовую стойку. Устройства резервного копирования поставляются с большой емкостью хранения и предварительно интегрированным программным обеспечением. Агенты резервного копирования устанавливаются в системы, для которых необходимо его выполнить, определяется расписание и политика копирования, и данные начинают передаваться на устройство резервного копирования. Как и в случае с другими вариантами, можно разместить устройство резервного копирования изолированно от локальной сети и, если есть возможность, на удаленном ресурсе.

Программные решения для резервного копирования сложнее развертывать и настраивать, чем аппаратные устройства, но они обеспечивают большую гибкость. Они позволяют определять, для каких систем и данных будет создаваться резервная копия, размещать резервные копии на выбранном устройстве хранения и автоматически управлять этим процессом.

Поставщики облачных услуг предлагают решения BaaS, в которых можно отправить локальные данные в общедоступное или частное «облако» и в случае аварии восстановить данные обратно из «облака». Решения BaaS просты в использовании и имеют большое преимущество в том, что данные хранятся в удаленном месте. Однако при использовании общедоступного «облака» необходимо обеспечить соблюдение соответствующих нормативных требований и стандартов и учитывать, что со временем затраты на хранение данных в «облаке» будут намного выше, чем затраты на развертывание аналогичного хранилища в локальной среде.

СТРАТЕГИЯ 3–2–1 РЕЗЕРВНОГО КОПИРОВАНИЯ ДЛЯ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ПРЕДПРИЯТИЯ

Авторами предложена стратегия 3–2–1 резервного копирования для критически важных информационных систем предприятия. Эта стратегия обеспечения адекватного дублирования систем и их надежного восстановления. Суть стратегии – три копии важных информационных систем предприятия создаются, как минимум, на двух разных носителях, и, по крайней мере, одна копия хранится удаленно.

Три копии данных включают исходные данные и два дубликата. Это гарантирует, что утерянная резервная копия или поврежденный носитель не повлияет на возможность восстановления.

Два разных типа хранения снижают риск сбоев, связанных с конкретным носителем, за счет использования двух разных технологий. Общие варианты включают внутренние и внешние жесткие диски, съемные носители или облачное хранилище.

При этом одна копия хранится непосредственно на предприятии. Инкрементальное или дифференциальное копирование проводится ежедневно. Имеются две резервные копии в разных удаленных местах («облако»). Раз в неделю делается полная копия дисков компьютера и отправляется в «облако» № 1. Дополнительно раз в месяц проводится еще одно полное копирование, результаты которого отправляются в «облако» № 2. Состав ежедневного и еженедельного набора постоянен. Таким образом, по сравнению с простой ротацией, в архиве содержатся только ежемесячные копии и последние еженедельные и ежедневные копии.

Одна удаленная копия устраняет риск, связанный с единой точкой отказа. Внешние дубликаты необходимы для надежных стратегий аварийного восстановления и резервного копирования данных, а при необходимости могут обеспечить аварийное переключение во время локальных сбоев.

РЕЗЕРВНОЕ КОПИРОВАНИЕ КРИТИЧЕСКИ ВАЖНЫХ ИТ-СИСТЕМ

Самый простой способ резервного копирования сервера – это решения, предложенные в [10, 11]. Это полное резервное копирование сервера. Оно может проводиться еженедельно, ежемесячно или ежеквартально и выполняться с использованием методов сжатия. Такие решения обычно предназначены для помощи в резервном копировании данных сервера на другой локальный сервер, облачный сервер или в гибридную систему. В частности, все более популярным становится резервное копирование в гибридные системы. Это связано с тем, что такие системы позволяют оптимизировать ресурсы, поддерживают простое дублирование в нескольких регионах и могут обеспечить более быстрое восстановление и переключение при отказе.

Как правило, решения для резервного копирования серверов должны включать следующие функции.

Поддержка различных типов файлов. Должны поддерживаться все виды файлов. В частности, решения должны поддерживать документы, электронные таблицы, мультимедийные файлы и файлы конфигурации.

Расположение резервной копии. Должна быть предусмотрена возможность указать места для резервной копии. Решение должно поддерживать резервное копирование в различные места и на различные носители, в том числе на внутренние и внешние ресурсы.

Планирование и автоматизация. Помимо возможности ручного резервного копирования, решения должны поддерживать автоматизацию резервного копирования посредством планирования. Это гарантирует, что у пользователя всегда будет последняя резервная копия и что резервные копии будут созданы согласованным образом.

Управление резервным копированием. Необходимо иметь возможность управлять жизненным циклом резервных копий, в том числе их количеством и продолжительностью хранения. В идеальном случае решения также позволяют легко экспортировать резервные копии для передачи на внешние ресурсы.

Выбор раздела. Разделы представляют собой изолированные сегменты ресурса хранения и часто используются для разделения данных в системе. Решения должны позволить пользователям самостоятельно создавать резервные копии данных и восстанавливать разделы.

Сжатие данных. Чтобы минимизировать объем хранилища, необходимый для многочисленных резервных копий, решения должны сжимать данные резервных копий. Это сжатие должно происходить без потерь и поддерживать целостность всех данных.

Выбор типа резервного копирования. Должна быть обеспечена возможность создания различных типов резервных копий, включая полные, дифференциальные и инкрементные. Дифференциальные резервные копии содержат копию изменений с момента последней полной резервной копии, в то время как инкрементальные – записи изменений с момента последней инкрементной резервной копии. Это может помочь уменьшить размер резервных копий и ускорить время резервного копирования.

Масштабирование. Возможности резервного копирования не должны ограничиваться объемом данных на серверах пользователей. Решения должны масштабироваться также, как и данные, и поддерживать резервные копии любого размера.

ТЕХНОЛОГИЯ РЕЗЕРВНОГО ХРАНИЛИЩА

Хранилище резервных копий – это физические места или устройства для хранения копий данных для восстановления в случае сбоя или потери данных. Системы хранения резервных копий обычно включают в себя как оборудование, так и программное обеспечение для управления копиями и восстановлением. Это включает в себя все: от простого флэш-накопителя до гибридной системы локального физического хранилища и удаленного облачного хранилища.

Какой бы метод ни использовался для резервного копирования, в конце концов, данные должны где-то храниться [12–14]. Технология, используемая для хранения данных резервного копирования, очень важна. Чем технология экономичнее, тем больше данных можно сохранить, и тем быстрее будут извлекаться эти данные. Чем надежнее технология хранения, тем будет больше гарантий сохранности резервных копий.

Сетевые ресурсы и NAS. Можно настроить централизованное хранилище, такое как сетевое хранилище (англ. network attached storage, NAS), сеть хранения данных (англ. storage area network, SAN) или обычные жесткие диски, подключенные как общий сетевой ресурс с использованием протокола сетевой файловой системы (англ. network file system, NFS). Это удобный вариант для предоставления локальным устройствам большого объема хранилища для резервного копирования. Однако он подвержен таким угрозам как пожар, наводнение и другим угрозам разрушения, затрагивающим весь центр обработки данных, а также кибератакам.

Облачное хранилище объектов. При использовании облачных провайдеров есть доступ к множеству сервисов хранения. Существуют инструменты, позволяющие автоматически создавать резервные копии данных, как из «облака», так и с локальных машин. Наиболее популярными являются:

AMANDA (англ. advanced maryland automatic network disk archiver) – система резервного копирования и архивирования информации.

Bacula – клиент-серверное программное обеспечение, позволяющее управлять резервным копированием, восстановлением и проверкой данных по сети для компьютеров и операционных систем различных типов.

Duplicity – производит резервное копирование в зашифрованные тома в tar-формате локально или на удаленный хост.

ЗАКЛЮЧЕНИЕ

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. Она защищает как от несчастных случаев, так и от вредоносных угроз, таких как программы-вымогатели, и обеспечивает надежное резервное копирование и восстановление данных.

Вклад авторов. Все авторы в равной степени внесли свой вклад в исследовательскую работу.

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

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. 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.

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
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.).

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, зашита. *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
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

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.).
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

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.

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.