ВЕСТНИК
ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
МОРСКОГО И РЕЧНОГО ФЛОТА ИМЕНИ АДМИРАЛА С. О. МАКАРОВА

DOI: 10.21821/2309-5180-2017-9-4-884-891

DATA BACKUP SYSTEM PLANNING

A. V. Chernyakov

Admiral Makarov State University of Maritime and Inland Shipping,
St. Petersburg, Russian Federation

In this paper studied the problem of digital data loss, presented actual means and methods of backup, storage and recovery of information, the analysis of the main metrics for designing a reliable data backup systems. A comprehensive study of this problem allows us to guarantee a long-term storage of critical information with guaranteed time of recovery on production sites with minimal downtime. Discussed the main causes of digital data loss and the impact of data corruption for organizations. Highlighted the main differences between backup mechanisms and archiving and long-term data storage. Examined the planning of the backup window, intermediate resource availability and providing necessary and sufficient characteristics of communication channels. Provided a list of organizational and technical means and measures that should be implemented when designing and operating a backup system to ensure its functioning. Examined the long-term storage problematic, the data recovery is impacted by the sizes of copies. Studied the influence of various factors, such as the use of different backup algorithms, the impact of encryption, deduplication and the use of different media on the speed of backup and restore operations. Discusses the advantages and disadvantages of classical backup algorithms, either separately or in combination. Given the analysis of the most common mistakes when planning backup and restore operations because of flaws in technical or organizational means.

Keywords: computing systems design, data backup technologies, data security, data storing systems, algorithms.

For citation:
Chernyakov, Arseniy V. "Data backup system planning." *Vestnik Gosudarstvennogo universiteta morskogo i rechnogo flota imeni admirala S. O. Makarova* 9.4 (2017): 884–891. DOI: 10.21821/2309-5180-2017-9-4-884-891.

УДК: 004.414.23

ПРОЕКТИРОВАНИЕ СИСТЕМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ ДАННЫХ

А. В. Черняков

ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова»,
Санкт-Петербург, Российская Федерация

В данной работе изучается проблема потери цифровых данных, дается характеристика актуальных методов резервного копирования, хранения и восстановления информации, приводится анализ основных метрик для проектирования надежных систем резервного копирования данных. Всестороннее изучение данной проблемы позволяет обеспечивать долгосрочное хранение критической информации с гарантированным временем восстановления на рабочие площадки с минимальным временем простоя. Рассматриваются главные причины потери цифровых данных и влияние потери данных на работу организаций. Приводятся главные отличия механизмов резервного копирования от механизмов архивирования и долгосрочного хранения данных. Изучаются вопросы планирования окна резервного копирования, промежуточной доступности ресурсов и обеспечения необходимых и достаточных характеристик каналов связи. Приводится перечень организационных и технических мер, которые должны осуществляться при проектировании и эксплуатации любой системы резервного копирования для обеспечения её бесперебойного функционирования. Для изучения проблемы долгосрочного хранения и быстрого восстановления данных производится наглядный анализ размеров создаваемых копий, детально рассматривается проблема быстрого роста итоговых объёмов репозиториев. Изучается влияние различных факторов, таких как использование различных алгоритмов резервного копирования, влияние шифрования, дедупликации и использование различных носителей информации на скорость операций резервного копирования и операций восстановления данных. Рассматриваются достоинства и недостатки классических алгоритмов резервного копирования как по отдельности, так и в комбинации. Производится разбор наиболее частых

ошибок при планировании систем резервного копирования и операций восстановления из-за недостатков технических или организационных средств.

Ключевые слова: проектирование вычислительных систем, технологии резервного копирования, безопасность информации, системы хранения данных, алгоритмы.

Для цитирования:
Черняков А. В. Проектирование системы резервного копирования данных / А. В. Черняков // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2017. — Т. 9. — № 4. — С. 884–891. DOI: 10.21821/2309-5180-2017-9-4-884-891.

Введение

В среднем объем хранимой и обрабатываемой информации различных деловых структур удваивается с интервалом в 1,2 года, и всё больше уникальной и критичной информации для их деятельности существует исключительно в электронном виде, выводя вопрос обеспечения её защиты на первый план [1], [2]. Причины, по которым происходит потеря данных, разнообразны. Наиболее частая причина — отказ оборудования в связи с механическими или электрическими повреждениями, ошибками контроллеров систем хранения данных — 44 % случаев. Почти каждый третий случай утраты связан с человеческим фактором (случайное удаление, неправильная эксплуатация систем хранения данных) — 32 %. Ошибки программного обеспечения при работе с файлами, при резервном копировании и восстановлении составляют 14 % от общего числа случаев потери данных. Вопреки распространённому мнению, компьютерные вирусы являются причиной утраты информации лишь в 7 % случаев, а на долю стихийных бедствий приходится и того меньше — 3 % [3].

Статистика демонстрирует важность защиты данных: после утраты критичной информации 80 % компаний объявляют себя банкротом в течение трех лет, 40 % из которых — в течение первого года. Скорость восстановления информации также играет большую роль: компании, которые не смогли восстановиться в течение 10 дней, в 93 % случаев объявляют банкротство в течение года, 50 % из которых — в течение первого месяца [4].

Несмотря на явную заинтересованность компаний в защите данных, опыт показывает, что их интересы в данной области, как правило, сводятся к одной из трех главных составляющих информационной безопасности, а именно, к конфиденциальности. Несомненно, конфиденциальность — наиболее деликатная тема для государственных учреждений и коммерческих компаний, производящих собственный продукт. Поэтому зачастую обеспечение должного уровня целостности и доступности информации не является определяющим в ходе формулирования требований ко многим информационным системам. Но в ряде случаев данные свойства информации будут являться превалирующими. Так, например, в транспортно-логистической отрасли потеря целостности и доступности информации приводит к существенным материальным убыткам, а в худшем случае — и к человеческим жертвам.

Абсолютной защиты не существует, но наиболее надёжным способом защиты информации от порчи или утраты является *резервное копирование* [5], [6]. Идея этого метода проста — данные, находящиеся в информационной системе, копируются на независимый носитель или дисковую систему, сохраняя, таким образом, своё состояние на определенный момент времени с целью восстановления в случае повреждения или утраты оригинала. Его не следует путать с архивированием — процедурой записи данных в архив для длительного хранения. Зачастую система резервного копирования создается по остаточному принципу — используются аппаратные средства с истекшим ресурсом службы, бывшие в ремонте или и вовсе не предназначенные для такого рода нагрузок (например, использование жестких дисков для персональных компьютеров с ограниченным ресурсом вместо серверных линеек). Так поступают по незнанию или из соображений экономии. Однако, как было отмечено, экономические последствия от неправильно спроектированной системы резервного копирования могут быть крупнее полученной выгоды. Подробный разбор экономической составляющей останется за переделами этой работы. Сосредоточимся на тезисе о незнании и устраним нехватку материалов по теме проектирования подобных систем.

В рамках данной работы рассматривается проектирование отказоустойчивых систем резервного копирования от сбора информации о системе и её емкостях до сопровождения в течение длительной эксплуатации, а именно применения различных алгоритмов резервного копирования и их влияния на размер репозитория копий и времени восстановления.

Методы и материалы

Для сокращения объема репозитория применяют различные алгоритмы резервного копирования. Наибольшей популярностью пользуются полное, инкрементное и дифференциальное резервирование [5]. Эти алгоритмы могут применяться как по отдельности, так и вместе. Кроме того, во избежание многократного сохранения одних и тех же данных, применяют метод дедупликации, заключающийся в исключении из резервной копии повторяющихся блоков данных и заменой их на ссылки [6].

Исследования эффективности алгоритмов показывают, какой объём при равных условиях занимают данные в репозитории резервных копий при использовании различных алгоритмов [7]. Так, наиболее требовательным к количеству доступного места является алгоритм полного резервного копирования из-за большого количества повторяющихся данных. Менее требовательным является алгоритм дифференциального копирования. Однако при отсутствии ротации копий, из-за большого количества измененных данных, может потребоваться больший объём системы хранения данных, чем при использовании полного архивирования. Наименее требовательным к дисковым ресурсам, а также наиболее быстрым при создании копии является алгоритм инкрементного копирования.

Метод многоуровневого резервного копирования основан на идее ротации резервных копий. Его ключевыми параметрами являются период резервирования, количество уровней и частота создания копий. На «нулевом» уровне создаётся полная резервная копия данных, на последующих — дифференциальные по отношению к предыдущему, или своему, уровню. Наиболее популярной является схема с тремя уровнями: полная резервная копия создаётся ежемесячно и хранится в течение года, дифференциальная копия первого уровня создаётся еженедельно и хранится один месяц, дифференциальная копия второго уровня создаётся ежедневно и хранится в течение недели. Это позволяет использовать самую сильную сторону дифференциального копирования — малый объём копий, сведя к минимуму недостаток — долгое время восстановления [8].

Предлагаемый алгоритм позволяет комплексно проанализировать инфраструктуру, выделить основные требования к системе, возможные ограничения, накладываемые средой, и эффективно внедрить разработанное решение. Проектирование системы резервного копирования можно условно разделить на два этапа, состоящих из нескольких шагов.

Этап 1 — административный

1. *Определение объёма копируемых данных*. Самым важным шагом можно по праву считать определение наиболее критичной информации, потеря которой может негативно или губительно сказаться на бизнес-процессах. Правильно проведя границу между ключевыми и вспомогательными данными, можно существенно сократить расходы на систему резервного копирования, уменьшив время снятия копий и требуемый объём дискового пространства.

2. *Задание частоты снятия копий*. На этом шаге необходимо определить минимальный отрезок времени, пропадание данных за который неприемлемо. Данный параметр целиком зависит от частоты изменения обозначенных данных. От него зависит не только объём репозитория резервных копий, но и версионность данных. Для каждого информационного актива этот параметр должен быть задан индивидуально.

3. *Оценка изменения данных*. Этот параметр выражает количественное изменение данных между операциями резервного копирования. Данный процент определяется экспериментально и служит основой для долгосрочного планирования объёма носителей и емкости интерфейсов системы резервного копирования.

4. *Определение допустимого времени снятия резервных копий.* Планирование так называемого «окна» резервного копирования, когда данные не используются или используются только для чтения. Это то время, в течение которого можно проводить резервное копирование. Чаще всего оно попадает на нерабочее время — вечер и ночь. В том случае, когда данные должны быть доступны для чтения и записи постоянно (системы высокой доступности), следует использовать специальные средства для копирования, такие как VSS, снэпшоты файловой системы [9].

5. *Определение необходимой ёмкости для системы резервного копирования*. Под ёмкостью понимается количество данных, которые система может принять во время окна копирования. Ёмкость вычисляется по формуле [10]:

$$C(\text{Гб}) = \sum_{\text{интерфейсов СРК}} w(\text{ч}) \cdot r\left(\frac{\text{МБ}}{\text{с}}\right) \cdot \frac{3600}{1000}, \quad (1)$$

где C — ёмкость СРК (ГБ); w — окно резервного копирования (ч); r — скорость передачи резервируемых данных с клиента в СРК (Гб/ч).

Если количество данных D, подлежащих резервному копированию в этот сеанс, превышает ёмкость системы, следует либо расширить систему за счет новых интерфейсов обмена, либо уменьшить количество данных, либо увеличить окно резервного копирования. В качестве r следует взять наименьшую из скоростей записи на носитель и скорости интерфейса обмена данными.

6. *Определение правил хранения резервных копий*. На этом шаге следует установить место хранения оперативной копии (это может быть система с низким временем доступа и высокой пропускной способностью, находящаяся в непосредственной близости от систем-клиентов), место хранения более старых, но актуальных копий: порядок помещения копии в архив, степень дедупликации, а также хранение копий в соответствии с политикой информационной безопасности предприятия и допуска сотрудников к хранилищам копий.

7. *Определение метода проверки резервных копий.* Если во время снятия копий произошла ошибка, она может остаться незамеченной вплоть до попытки восстановления из этой копии. Проверка чаще всего осуществляется математическими методами самого́ программного обеспечения системы резервного копирования, но наиболее надёжным является метод восстановления данных «в песочнице» для проверки их целостности. Этот шаг призван регламентировать методы защиты от ошибок.

8. *Определение метода утилизации носителей.* Носители с истекшим сроком годности могут быть помещены в архив, а могут быть утилизированы. На этом шаге следует указать метод уничтожения неактуальных резервных копий. Он должен быть согласован с политикой информационной безопасности предприятия.

Этап 2 — проектирование (анализ имеющейся) системы резервного копирования

1. *Определение пропускной способности интерфейса системы резервного копирования*. Необходимая скорость получения данных для завершения создания копии, не выходя за рамки окна резервного копирования, вычисляется как отношение объема копируемых данных D к окну резервного копирования w. Если система резервного копирования осуществляет связь с клиентами по сети, необходимо учитывать пропускную способность канала, которая будет равна пропускной способности наименее производительного участка. Формула (2) иллюстрирует сравнение пропускной способности интерфейса B с необходимой скоростью получения данных R_n:

$$R_n\left(\frac{\text{Гб}}{\text{ч}}\right) \cdot 8 \le B\left(\frac{\text{Мбит}}{\text{с}}\right) \cdot \frac{3600}{1000}, \quad (2)$$

где R_n — необходимая скорость передачи резервируемых данных (Гб/ч); B — пропускная полоса канала передачи данных (Мбит/с).

Если неравенство не выполняется, то имеющаяся среда передачи данных не обеспечивает достаточной скорости передачи информации.

2. *Определение пропускной способности интерфейса клиента системысистемы*, т. е. скорости, с которой клиент системы резервного копирования может принимать и получать от неё данные. Равна наименьшей из скоростей чтения / записи запоминающего устройства или канала передачи информации.

3. *Выбор оптимального алгоритма снятия резервных копий*. От выбора алгоритма резервного копирования зависит очень многое, в частности время копирования и восстановления, объём передаваемых данных, объём репозитория резервных копий, метод их хранения. Эти вопросы были уже рассмотрены в статье.

4. *Определение времени снятия и восстановления копий* (включает в себя время чтения и записи, пропускную способность канала). На этом шаге определяется реальная скорость копирования и восстановления данных. В случае, если время превышает допустимое, проводится структурный анализ системы резервного копирования и принимается решение о добавлении новых промежуточных узлов или использовании более быстрого канала.

Результаты

Для наглядного представления приведенных методов рассмотрим следующую ситуацию: первоначальный объём данных D_0 равен 100 ГБ, период снятия резервных копий d составляет один день, между операциями резервного копирования изменяется 5 % данных (модификатор $p = 0{,}05$). Для многоуровневой схемы установим следующее расписание ротации: полное резервное копирование осуществляется один раз в 14 дней, дифференциальное по отношению к полному — один раз в 7 дней, инкрементное по отношению к предыдущей копии — ежедневно. Объём данных D_n через n дней вычисляется по формуле

$$D_n = (1 + p)^n D_0, \tag{3}$$

где D_n — объём данных, подлежащих копированию, к n-му дню, Гб; D_0 — начальный объём данных для копирования, Гб; p — модификатор изменения данных.

Проиллюстрируем объём создаваемой резервной копии при четырех схемах резервного копирования при помощи данных, приведенных в таблице.

Сравнение объёма резервной копии снятой различными алгоритмами, Гб

День	D_n	Full	Diff	Inc	ML3
0	100,00	100,00	100,00	100,00	100,00
1	105,00	105,00	5,00	5,00	5,00
2	110,25	110,25	10,25	5,25	5,25
3	115,76	115,76	15,76	5,51	10,51
4	121,55	121,55	21,55	5,79	11,04
5	127,63	127,63	27,63	6,08	16,59
6	134,01	134,01	34,01	6,38	17,42
7	140,71	140,71	40,71	6,70	40,71
8	147,75	147,75	47,75	7,04	24,46
9	155,13	155,13	55,13	7,39	30,68
10	162,89	162,89	62,89	7,76	32,21
11	171,03	171,03	71,03	8,14	38,82
12	179,59	179,59	79,59	8,55	40,76
13	188,56	188,56	88,56	8,98	47,80
14	197,99	197,99	97,99	9,43	197,99
Итого		**2 057,86**	**657,86**	**97,99**	**320,57**

Обсуждение

Проведем сравнительный анализ результатов. Наглядно показано, что алгоритм полного копирования сохраняет большое количество дублируемой информации, в результате чего объём репозитория растет очень быстро. Дифференциальный подход показывает хороший результат на коротком промежутке, начиная с 5 % объёма полной резервной копии, но уже к концу 14-го дня дифференциальная копия составляет около 50 % от полной. Инкрементный алгоритм является наилучшим с точки зрения экономии ресурсов при создании копий, однако легко показать, что он обладает более низкой надёжностью по сравнению с указанными. Из-за отсутствия избыточности данных, при утрате одной копии в цепочке их восстановление становится невозможным. Использование всех трех алгоритмов в многоуровневой схеме показывает хороший результат по времени копирования и требуемому объёму. Недостатком является неравномерное использование системы резервного копирования (при переходе на нижележащий уровень количество копируемых данных возрастает по отношению к верхним уровням). Это может негативно сказаться на планировании окна резервного копирования [11].

Для организации надежной системы резервного копирования требуется составить перечень информационных ресурсов, подлежащих защите, приоритезировать резервное копирование критичной информации, задать время хранения и частоту создания копий, определить меры безопасности по пресечению неавторизированного доступа, рассчитать необходимый размер репозитория для долгосрочного и оперативного хранения информации.

Для обеспечения безопасности данных при снятии резервных копий практикуется их шифрование. Зашифрованные данные, как правило, занимают больший объём, плохо поддаются сжатию, а их восстановление занимает больше времени и требует бóльших вычислительных ресурсов, чем не зашифрованные, однако оно позволяет избежать рисков кражи или подмены информации в репозитории. Зачастую шифровать все данные не требуется, достаточно обеспечить защиту наиболее критичной информации [12].

При проектировании систем резервного копирования обязательным шагом является составление расписания ротации резервных копий, что позволяет гибко распределить ресурсы системы резервного копирования. Так, оперативная копия может храниться на серверах с высокой доступностью, архивные копии — на сторонних носителях: оптических дисках, ленточных накопителях или на вспомогательных серверах. Количество оперативных и архивных копий следует рассчитать с учётом требований ко времени восстановления и продолжительности хранения информации. Кроме того, следует учитывать доступный объём системы хранения данных, определенной для архива и репозитория.

Для определения требований к технической базе системы резервного копирования может применяться подход, лежащий в основе систем управления жизненным циклом информации (Information Lifecycle Management, ILM), который постулирует динамичность ценности информации на основе её актуальности в бизнес-процессах. С его помощью можно отделить критичные данные, требующие высокой скорости доступа, частого резервирования и быстрого восстановления, от более простых и менее критичных данных, расположив их на разных технических площадках [13].

Заключение

Приведенный план позволяет формализовать требования и спроектировать надёжную систему резервного копирования. Это особенно актуально на крупных предприятиях стратегического значения, какими являются транспортно-логистические кластеры и их отдельные составляющие: аэро- и морские порты, грузовые и пассажирские хабы и многие другие предприятия транспортной отрасли, от бесперебойного функционирования которых зависит экономика.

Тема резервного копирования настолько же важна, насколько и обширна. Она охватывает множество аспектов взаимодействия человека и вычислительной техники, обеспечивая защиту от порчи или утраты интеллектуального труда или иных данных, хранящихся в цифровом виде. Ошибки, допущенные при проектировании систем резервного копирования, могут привести к по-

тере данных, компенсировать которую сможет не каждая компания. Некачественный или редкий аудит системы может дать ложное ощущение безопасности.

Для проектирования надежной системы необходимо выполнить комплекс административно-технических мер по приоритезации информационных активов, анализу окружения, планированию расписания резервирования, созданию регламентирующих процедур и документов. Освещаемые в статье вопросы помогут собрать необходимые данные о среде и подготовить базу для создания надежной системы резервного копирования.

СПИСОК ЛИТЕРАТУРЫ

1. Australian organizations facing acute threat of cyber-attack [Электронный ресурс]. — Режим доступа: www.bsigroup.com/en-AU/About-BSI/Media-Centre/Press-Releases/2013-News/November/Australian-Organizations-Facing--Acute-Threat-Of-Cyber-Attacks/ (дата обращения: 21.12.2016).

2. *Nyrkov A. P.* Providing the integrity and availability in the process of data transfer in the electronic documents management systems of transport-logistical clusters / A. P. Nyrkov, S. S. Sokolov, S. G. Chernyi, A. V. Chernyakov, A. S. Karpina // Industrial Engineering, Applications and Manufacturing (ICIEAM), International Conference on. — IEEE, 2016. — Pp. 1–4. DOI: 10.1109/ICIEAM.2016.7910915.

3. Avoiding the hidden costs of the Cloud [Электронный ресурс]. — Режим доступа: http://www.symantec.com/content/en/us/about/media/pdfs/b-state-of-cloud-global-results-2013.en-us.pdf (дата обращения: 17.06.2016).

4. SaaS Data Loss: The Problem You Didn't Know You Had [Электронный ресурс]. — Режим доступа: http://resources.healthdatamanagement.com/content28634 (Дата обращения: 17.06.2016).

5. *Черняков А. В.* Алгоритмы резервного копирования / А. В. Черняков, А. П. Нырков // IT: вчера, сегодня, завтра: материалы III науч.-исслед. конф. факультета информационных технологий. — СПб.: Изд-во ГУМРФ им. адм. С. О. Макарова, 2015. — С. 129–133.

6. *Нырков А. П.* Дедупликация данных в системах резервного копирования / А. П. Нырков, А. В. Черняков // Информационные управляющие системы и технологии: материалы IV Междунар. науч.-практ. конф. (ИУСТ-ОДЕССА-2015). — Одесса, 2015. — С. 130–133.

7. *Chervenak A.* Evaluating Backup Algorithms / A. Chervenak, Z. Kurmas / Proceedings of the Eighth Goddard Conference on Mass Storage Systems and Technologies. — USA, Maryland, 2000. — Pp. 235–242.

8. *Joanna O.* Multilevel backups / O. Joanna, S. Stafford, A. Weeks, L. Wizenius // The Linux System Administrator's Guide. — USA, 2004. — Pp. 83–89.

9. *Черняков А. В.* Механизмы защиты данных в файловых системах / А. В. Черняков, А. П. Нырков // IT: ВЧЕРА, СЕГОДНЯ, ЗАВТРА: материалы IV науч.-исслед. конф. студентов и аспирантов Института водного транспорта. — СПб.: Изд-во ГУМРФ им. адм. С. О. Макарова, 2016. — С. 291–296.

10. Handbook of Network and System Administration / J. Bergstra, M. Burgess, eds. — 1st Edition. — Elsevier, 2007. — 1016 p.

11. *Ranjith G.* A Multiple Segmented Backups Scheme for Dependable Real-time Communication in Multihop Networks / G. Ranjith, C. Siva Ram Murthy // Proceedings of The International Parallel and Distributed Processing Symposium. — USA, 2003. — Pp. 123–130.

12. *Нырков А. П.* Алгоритмы резервного копирования для обеспечения защиты данных / А. П. Нырков, А. В. Черняков // Информационная безопасность регионов России (ИБРР-2015): материалы конф. — СПб.: Изд-во СПОИСУ, 2015. — С. 127–128.

13. *Stephens D.* Records Management: Making the Transition from Paper to Electronic / D. Stephens. — Overland Park, KS: ARMA International, 2007. — 292 p.

REFERENCES

1. Australian organizations facing acute threat of cyber-attack. Web. 21 Dec. 2016 <www.bsigroup.com/en-AU/About-BSI/Media-Centre/Press-Releases/2013-News/November/Australian-Organizations-Facing--Acute-Threat-Of-Cyber-Attacks/>.

2. Nyrkov, A., S. Sokolov, S. Chernyi, A. Chernyakov, and A. Karpina. "Providing the integrity and availability in the process of data transfer in the electronic documents management systems of transport-logistical clus-

ters." *Industrial Engineering, Applications and Manufacturing (ICIEAM), International Conference on*. IEEE, 2016. DOI: 10.1109/ICIEAM.2016.7910915.

3. Avoiding the hidden costs of the Cloud. Web. 17 June 2016 <www.symantec.com/content/en/us/about/media/pdfs/b-state-of-cloud-global-results-2013.en-us.pdf>

4. SaaS Data Loss: The Problem You Didn't Know You Had. Web. 17 June 2016 <resources.healthdatamanagement.com/content28634>.

5. Chernyakov, A. V., and A. P. Nyrkov. "Algoritmy rezervnogo kopirovaniya." *IT: vchera, segodnya, zavtra Materialy III nauchno-issledovatel'skoi konferentsii fakul'teta informatsionnykh tekhnologii*. SPb.: GUMRF imeni admirala S.O. Makarova, 2015. — S. 129–133.

6. Nyrkov, A. P., and A. V. Chernyakov. "Deduplikatsiya dannykh v sistemakh rezervnogo kopirovaniya." *Informatsionnye upravlyayushchie sistemy i tekhnologii Materialy IV Mezhdunarodnoi nauchno-prakticheskoi konferentsii (IUST-ODESSA-2015)*. Odessa, 2015: 130–133.

7. Chervenak, A., and Z. Kurmas. "Evaluating Backup Algorithms." *Proceedings of the Eighth Goddard Conference on Mass Storage Systems and Technologies*. USA, Maryland, 2000: 235–242.

8. Joanna, O., S. Stafford, A. Weeks, and L. Wizenius. "Multilevel backups." *The Linux System Administrator's Guide*. USA, 2004: 83–89.

9. Chernyakov, A. V., and A. P. Nyrkov. "Mekhanizmy zashchity dannykh v failovykh sistemakh." *IT: VCh-ERA, SEGODNYa, ZAVTRA: Materialy IV nauchno-issledovatel'skoi konferentsii studentov i aspirantov Instituta vodnogo transporta*. SPb.: GUMRF imeni admirala S.O. Makarova, 2016: 291–296.

10. Bergstra, J., and M. Burgess, eds. *Handbook of Network and System Administration*. 1st Edition. Elsevier, 2007.

11. Ranjith, G., and C. Siva Ram Murthy. "A Multiple Segmented Backups Scheme for Dependable Real-time Communication in Multihop Networks." *Proceedings of The International Parallel and Distributed Processing Symposium*. USA, 2003: 123–130.

12. Nyrkov, A. P., and A. V. Chernyakov. "Algoritmy rezervnogo kopirovaniya dlya obespecheniya zashchity dannykh." *Information security of Russian regions (ISRR-2015). IX St. Petersburg interregional conference*. St. Petersburg, 2015: 127–128.

13. Stephens, D. *Records Management: Making the Transition from Paper to Electronic*. Overland Park, KS: ARMA International, 2007.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Черняков Арсений Вениаминович — аспирант
Научный руководитель:
Нырков Анатолий Павлович — доктор технических наук, профессор
ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова»
198035, Российская Федерация, Санкт-Петербург, ул. Двинская, 5/7
e-mail: *m@avc.su*, *kaf_koib@gumrf.ru*

INFORMATION ABOUT THE AUTHOR

Chernyakov, Arseniy V. — Postgraduate
Supervisor:
Nyrkov, Anatoliy P. —
Dr. of Technical Sciences, professor
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya Str., St. Petersburg 198035, Russian Federation
e-mail: *m@avc.su*, *kaf_koib@gumrf.ru*

Статья поступила в редакцию 15 июля 2017 г.
Received: July 15, 2017.