DOI https://doi.org/10.15407/usim.2019.02.080
УДК 004.9:004.75

Ю.М. ЛИСЕЦКИЙ, д-р техн. наук, генеральный директор,
ДП «ЭС ЭНД ТИ УКРАИНА», просп. Академика Палладина, 44,
Киев, 03680, Украина,
Yurii.Lysetskyi@snt.ua

С.В. КОЗАЧЕНКО, инженер по обслуживанию платформ и операционных систем,
ДП «ЭС ЭНД ТИ УКРАИНА», просп. Академика Палладина, 44,
Киев, 03680, Украина,
Saveliy.Kozachenko@snt.ua

РЕЗЕРВНОЕ КОПИРОВАНИЕ КАК ИНСТРУМЕНТ ЗАЩИТЫ ИНФОРМАЦИИ

Рассмотрены основные системы резервного копирования и их особенности. Описана технология контроля и мониторинга виртуальных и физических систем, обеспечивающая распределение заданий резервного копирования и автоматическую защиту новых виртуальных систем и технология дедупликации, позволяющая устранить дублирование данных и сократить при этом количество физических носителей для их хранения.

Ключевые слова: *данные, защита информации, резервное копирование, восстановление, информационно-технологическая инфраструктура, технология, дедупликация, виртуальные машины.*

Введение

Существует достаточно большое количество определений термина информация, так как в понятие «информация» вкладывается различный смысл в зависимости от предметной области, для которой оно рассматривается [1]. Обычно под информацией подразумевают любые сведения (сообщения, данные) независимо от формы их представления. К основным видам информации относятся: графическая, звуковая, текстовая, числовая и видеоинформация, которые определяются формой ее представления, а также способами кодирования и хранения. С точки зрения информатики наиболее важные свойства информации — актуальность, целостность, достоверность, аутентичность, конфиденциальность и доступность [1].

С ростом объемов информации, находящейся на различных носителях, устройствах и системах, усложняется задача надежности их хранения, особенно в современных условиях вирусной активности, информационных угроз, кибератак [2–5]. Один из инструментов защиты информации — резервное копирование и создание информационных архивов для быстрого доступа к данным [6]. Для этого необходимо иметь механизмы их быстрого восстановления из резервных копий. Традиционные методы архивирования и восстановления — малоэффективны и не позволяют реализовать требования по надежной сохранности и доступности информации. Решить эту задачу можно с помощью систем резервного копирования [7].

Основные системы резервного копирования и их особенности

На сегодняшний день существует большое количество промышленных систем резервного копирования с различным функционалом. Из них можно выделить основных производителей, системы которых максимально соответствуют современным требованиям к хранению информации. Это компании *IBM* с *Tivoli Storage Manager, EMC* с *Neworker* и *Avamar, Veritas* с *Backup Exec* и *NetBackup*, которая является лидером в этом сегменте.

Tivoli Storage Manager — это система резервного копирования уровня предприятия. Предоставляет автоматизированные сервисы управлением данными на рабочих станциях и серверах, работающих на различных операционных системах (ОС). Для интерактивного резервного копирования применяется *программа-клиент*, инициирующая резервное копирование или восстановление данных. В своем составе имеет различные компоненты, позволяющие наращивать необходимый функционал для различного рода задач. Как правило, *Tivoli Storage Manager* используют в составе комплексных решений на базе аппаратного и программного обеспечения (ПО) от *IBM*.

Neworker и ***Avamar*** в основном ориентированы на работу с программно-аппаратным обеспечением их разработчика компании *EMC*, так как полностью совместимы со всеми системами, которые она производит и достаточно просто с ними интегрируются. Поэтому если в информационно-технологической инфраструктуре (ИТИ) используются системы хранения данных (СХД) от *EMC*, то в этом случае *Neworker* и *Avamar* будут наиболее эффективными для решения задач резервного копирования данных.

Backup Exec и *NetBackup* — первый ориентирован на малые и средние предприятия, в ИТИ которых преобладают ОС на базе *Windows*, а второй предназначен для защиты данных в *enterprise*-сегменте с гетерогенной ИТИ. Это комплексные решения, позволяющие выполнять все возможные виды резервного копирования, начиная от отдельных физических или виртуальных систем, заканчивая восстановлением приложений и баз данных (БД) в масштабах всего предприятия. Эти системы резервного копирования работают на основе технологии *V-Ray*.

Технология V-Ray

Технология *V-Ray* представляет собой новый уровень контроля и мониторинга виртуальных и физических систем, которая обеспечивает распределение заданий резервного копирования и автоматическую защиту новых виртуальных систем по мере их подключения. Она предоставляет возможность контролировать виртуальные файловые системы и приложения с дальнейшим выполнением прозрачного резервного копирования, применяя гибкие варианты технологии дедупликации файлов, которая в свою очередь позволяет существенно сократить объем резервной копии на СХД. Благодаря встроенной интеллектуальной дедупликации появилась возможность повысить эффективность хранения данных до 98 процентов и сократить объем резервных копий *VMware* и *Hyper-V* до 95 процентов. Технология *V-Ray* существенно экономит время на резервное копирование и восстановление в распределенной ИТИ, а также упрощает управление этими процессами.

Для виртуальной среды технология *V-Ray* дает возможность обеспечить безопасность, защиту, резервное копирование и восстановление данных в любой момент времени и в любом месте. Благодаря этой технологии можно уменьшить нагрузку на сеть и СХД, а также быстрее восстанавливать данные без снижения производительности виртуальной среды, так как для ее работы не требуются агенты. *V-Ray* позволяет восстановить нужные данные всего за несколько минут путем использования технологии гранулярного восстановления, которая исключает необходимость длительного поиска архива в СХД для обнаружения нужного файла. Для этого реализована возможность прямого обращения к *backup*-образам систем

с целью выбора и восстановления нужной информации. Технология *V-Ray* автоматически защищает новые виртуальные машины, которые перешли в состояние *online*, при этом политика резервного копирования остается неизмененной.

Технология дедупликации

Дедупликация данных — это технология, позволяющая устранить дублирование данных и сократить при этом объёмы физических носителей для хранения. До ее появления каждая резервная копия могла иметь одинаковый набор неизменившихся файлов со времени последней резервной копии, что приводило к увеличению объемов хранения, а с ростом изменяемых данных увеличивало и время резервного копирования.

Технология работает на уровне блоков данных, записанных на диск, где используются хеш-функции. Когда система дедупликации находит совпадающие хеш-функции для разных блоков, она предлагает сохранить блоки в виде единственного экземпляра и набора ссылок на него.

Эта технология также позволяет проводить глобальную дедупликацию — сравнивать блоки данных с разных компьютеров, что еще больше увеличивает эффективность дедупликации, так как на дисках разных компьютеров с одной и той же ОС может храниться большое количество повторяющихся данных. В системах резервного копирования компании *Veritas* реализованы три способа применения дедупликации:

- *дедупликация на стороне клиента/источника* при которой в СХД передаются только уникальные данные, при этом сервер резервного копирования в процессе не участвует, что позволяет освободить его ресурсы для выполнения других задач и снизить нагрузку на каналы передачи;
- *дедупликация на сервере*, при которой данные, поступающие на систему резервного копирования, дедуплицируются и записываются на СХД;
- *дедупликация на устройстве*, при которой данные дедуплицируются непосредственно на СХД, с которыми интегрированы системы резервного копирования, что позволяет быстро восстанавливать данные путем минимизации времени восстановления (*recovery time objec tive — RTO*) в случае сбоя.

Особенно эффективной технология дедупликации показала себя в виртуальных инфраструктурах *VMware* и *Hyper-V*, где большинство таких ОС, как *Windows* и *Linux*, развернуты с эталонного дистрибутива и содержат одинаковый набор программ, компонент и библиотек на своих виртуальных дисках и могут отличаться между собой только файлами и папками персональных настроек. Каждая такая виртуальная машина занимает десятки гигабайт в системе хранения, и в этом случае технология дедупликации помогает уменьшить объем резервных копий и сократить время на их создание. Использование этих технологий позволяет ускорить резервное копирование до 10 раз, а объем резервных копий сократить на 95 процентов.

Система резервного копирования Backup Exec

Наиболее распространенной системой резервного копирования есть *Backup Exec*, способная защитить не только физические среды, но и виртуальные. Многофункциональность *Backup Exec* позволяет реализовать всевозможные сценарии работы с такими объектами ИТИ организации, как виртуальные машины, физические серверы, приложения, их компоненты, файлы, папки (рис. 1). Основные преимущества *Backup Exec*:

- резервное копирование на любые устройства хранения, такие как жесткий диск, ленточные библиотеки, хранилища, доступные по *SAN* или *LAN*, облачные сервисы *Amazon S*3, *Google Cloud Storage* и *Microsoft Azure*;
- быстрое создание моментальных копий виртуальных машин с учетом тесной интеграции с *Microsoft Volume Shadow Copy Service* (*VSS*) и *VMware vStorage API for Data Protection*

(*VADP*), что позволяет уменьшить потребление ресурсов процессора, памяти ввода-вывода на виртуальной машине;

▪защита виртуальных машин с *Microsoft Exchange, Microsoft SharePoint, Microsoft Active Directory, Microsoft SQL Server* благодаря встроенной функции *Instant Granular Recovery Technology* (*GRT*), которая позволяет из резервных копий виртуальных машин мгновенно извлекать и восстанавливать отдельные файлы, папки, БД *SQL*, хранилища *Exchange* и элементы почтовых ящиков;

▪ интегрированная функция восстановления после аварии — технология *Bare Metal Restore*, встроенная в процесс резервного копирования, способна выполнить восстановление на исходную аппаратную платформу либо на отличную от нее (рис.1).

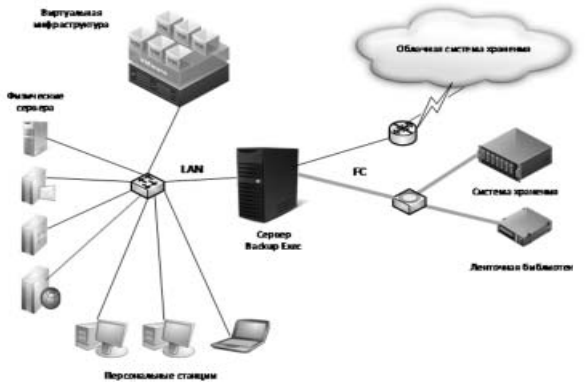

Рис. 1. Интеграция *Backup Exec* с объектами ИТИ

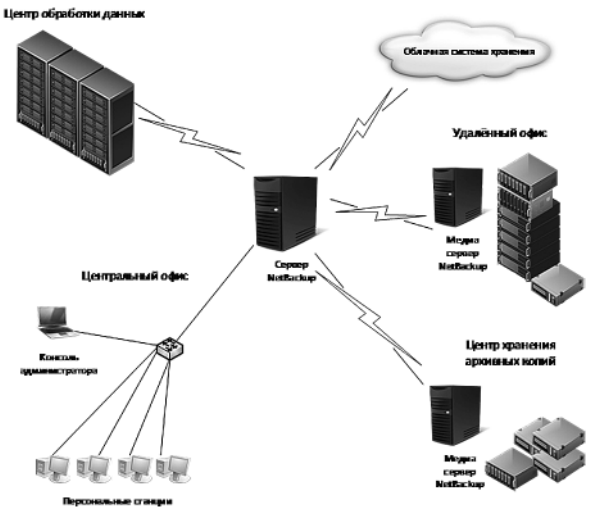

Рис. 2. Интеграция *NetBackup* с объектами ИТИ

Система резервного копирования NetBackup

Это кроссплатформенное решение для резервного копирования, способное работать с очень большими объемами данных для комплексной защиты физических и виртуальных систем, приложений и БД в корпоративных центрах обработки данных (ЦОД). Система обладает высоким уровнем производительности, автоматизации и масштабируемости, ориентирована на организации корпоративного уровня, ИТИ которых включает в себя тысячи как физических, так и виртуальных серверов (рис. 2). В ее состав включен широкий набор компонент для оптимизации резервного копирования и восстановления в гетерогенных средах, позволяющих работать с такими ОС, как *HP-UX, HP Tru64, IBM AIX, Linux, Microsoft Windows, Novell NetWare, SGI IRIX* и *Sun Solaris*. Для оперативного восстановления критически важных БД и приложений *NetBackup* предлагает агентов для взаимодействия с программным и аппаратным обеспечением компаний *IBM, Microsoft, Oracle, SAP* и *Sybase*.

Система резервного копирования *NetBackup* в своей стандартной конфигурации имеет трехуровневую архитектуру.

Мастер-сервер — обеспечивает централизованное управление всей инфраструктурой резервного копирования. Администратор может с одной консоли управлять всеми носителями резервного копирования, создавать политики, задавать и управлять расписанием резервного копирования, создавать отчеты по результатам операций.

Медиа-сервер — отвечает за работу с ленточными или дисковыми СХД, которых в защищаемой инфраструктуре, как правило, несколько, и каждый может работать как с одним, так и с несколькими типами различных СХД, что позволяет повысить скорость записи резервных копий через медиа-серверы с ба-

лансировкой между ними трафика резервного копирования.

Агент — клиентская программа, обеспечивающая чтение и отправку данных с защищаемых серверов.

К основным преимуществам *NetBackup* относятся:

- *централизованное управление* — управление всеми серверами *NetBackup* из одной консоли управления, что позволяет повысить эффективность системы;
- *высокая производительность* — использование технологии синтетического резервного копирования позволяет сохранить пропускную способность сети и снизить уровень влияния на сервер приложения благодаря тому, что резервное копирование выполняется только один раз, а также мультиплексирование — до 32 различных потоков данных на один ленточный накопитель обеспечивает максимальную пропускную способность аппаратного обеспечения для хранения информации;
- *автоматизированное аварийное восстановление* — с помощью технологии *Bare Metal Restore* обеспечивает восстановление системы и возобновление работоспособности серверов в случае аварийной ситуации;
- *NetBackup Vault Option* — управление удаленными ленточными накопителями, используется для создания и хранения дубликатов ленточных носителей на резервной площадке. Система резервного копирования *NetBackup* также имеет дополнительный функционал, расширяющий ее возможности.

NetBackup Accelerator for VMware — функция, позволяющая сократить время, необходимое для резервного копирования виртуальных машин путем комбинирования инкрементального резервного копирования с дедупликацией.

После выполнения полного резервного копирования на дисковую библиотеку передаются только измененные блоки, используется механизм отслеживания измененных блоков *VMware Changed Block Tracking* (*CBT*), а затем медиа-сервер собирает из инкрементальных резервных копий полную копию с помощью функции синтетического резервного копирования *Optimized Synthetics*.

NetBackup Accelerator for Microsoft Hyper-V — функция, практически аналогична *NetBackup Accelerator for VMware*, но в отличие от нее резервное копирование выполняется с помощью технологии *Microsoft Resilient Change Tracking* (*RCT*), встроенной в *Windows Server* 2016. Осуществляется передача только измененных блоков и синтез новых полных резервных копий, резервное копирование и восстановление виртуальных машин *Hyper-V* в этом случае можно выполнять в значительно меньший промежуток времени.

NetBackup for vCloud Director — интеграция с *Vmware vCloud Director* позволяет с помощью этой функции обнаруживать развернутые в публичном или частном облаке новые виртуальные машины и сразу обеспечивать их защиту. Даже если образы виртуальных машин достигают объема 2 ТБ, *NetBackup* обладает возможностью их восстановления в течение нескольких минут.

Таким образом, система резервного копирования *Backup Exec* ориентирована на использование организациями в ИТИ, основные сервисы которых работают под управлением ОС *Windows* и резервное копирование которых выполняется на несколько устройств хранения, в отведенное для этого ночное время и не требует для этого дополнительных ресурсов. Использование системы резервного копирования *NetBackup* будет более эффективным в организациях корпоративного уровня с гетерогенной ИТИ, в которых сервисы работают под различными ОС (*Unix, Linux, Windows*), с большими объемами данных и для резервного копирования которых необходимы более гибкие инструменты и настройки.

Заключение

В статье рассмотрены основные системы резервного копирования и их особенности. Описана технология контроля и мониторинга виртуальных и физических систем, обеспечивающая распределение заданий резервного

копирования и автоматическую защиту новых виртуальных систем и технология дедупликации, позволяющая устранить дублирование данных и сократить при этом количество физических носителей для их хранения. Проведен анализ наиболее распространённых систем резервного копирования *Backup Exec* и *NetBackup*, исследованы их преимущества и недостатки, а также приведены рекомендации по практическому использованию.

Таким образом, системы резервного копирования — критически важный элемент ИТИ любой организации и эффективный инструмент обеспечения защиты информации.

ЛИТЕРАТУРА

1. Понятие информации, ее виды и свойства, https://spravochnik.ru/informatika/informacionnye_processy_i_informaciya/ponyatie_informacii_eevidy_i_svoystva/
2. *Анин Б.Ю.* Защита компьютерной информации. СПб.: BHV-Санкт-Петербург, 2000. 384 с.
3. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных. Кн. 1. М.: Энергоатомиздат, 1994. 400 с.
4. *Лисецкий Ю.М.* Информационная безопасность: защита от DDoS-атак. 16-th Int. Conf. «System Analysis and Information Technologies SAIT 2014», (Київ, 26–30 May 2014). Kyiv, 2014. P. 405–406.
5. *Лисецкий Ю.М., Бобров С.И.* Новые угрозы информационной безопасности или оружие массового заражения. Математичні машини і системи. 2018. № 1. С. 41–50.
6. *Бережной А.Н.* Сохранение данных: теория и практика. М.: ДМК Пресс, 2016. 317 с.
7. *Лисецкий Ю.М.* Защита информации: системы резервного копирования. 20-th Int. Conf. «System Analysis and Information Technologies SAIT 2014», (Київ, 21–24 May 2018). Kyiv, 2018. P. 236–237.

Поступила 06.03.2019

REFERENCES

1. *The concept of information*, its types and properties, https://spravochnik.ru/informatika/informacionnye_processy_i_informaciya/ponyatie_informacii_eevidy_i_svoystva/ (In Russian).
2. *Anin, B.Yu.*, 2000. Zashchita kompyuternoy informatsii. SPb.: BHV-Sankt-Peterburg, 384 p. (In Russian).
3. *Gerasimenko, V.A.*, 1994. Zashchita informatsii v avtomatizirovannykh sistemakh obrabotki dannykh. Kn. 1. M.: Energoatomizdat, 400 p. (In Russian).
4. *Lisetskiy, Yu.M.*, 2014. "Informatsionnaya bezopasnost': zashchita ot DDoS-atak". 16-th Int. Conf. System Analysis and Information Technologies SAIT 2014, (Kiyv, 26–30 May 2014). Kyiv, 2014, pp. 405–406. (In Ukrainian).
5. *Lisetskiy, Yu.M.*, *Bobrov S.I.,* 2018. "Novyye ugrozy informatsionnoy bezopasnosti ili oruzhiye massovogo zarazheniya". Matematychni mashyny i systemy, 1, pp. 41–50. (In Russian).
6. *Berezhnoy, A.N.*, 2016. Sokhraneniye dannykh: teoriya i praktika. M.: DMK Press, 317 p. (In Russian).
7. *Lisetskiy, Yu.M.*, 2018. "Zashchita informatsii: sistemy rezervnogo kopirovaniya". 20-th Int. Conf. System Analysis and Information Technologies SAIT 2014, (Kiyv, 21–24 May 2018). Kyiv, pp. 236–237. (In Ukrainian).

Received 06.03.2019

YU.M. Lisetsky, Doctor of Technical Sciences, General Director,
DP «S&T UKRAINE»,
Prosp. Akad. Palladina, 03680, Kiev, Ukraine 44,
Iurii.Lysetskyi@snt.ua

S.V. Kozachenko, Platforms & Operating Systems Engineer,
DP «S&T UKRAINE»,
Prosp. Akad. Palladina, 03680, Kiev, Ukraine 44,
Saveliy.Kozachenko@snt.ua

BACKUP COPYING AS THE INFORMATION PROTECTION TOOL

Introduction. As the volumes of information stored to different storage devices steadily grow, the issue of storage reliability becomes more and more complicated. One of the information protection tools is the backup copying and creation of information archives for quick data access.

Main Backup Systems and their Features. Major manufacturers of modern backup systems are IBM offering Tivoli Storage Manager, EMC offering Neworker and Avamar, Veritas offering Backup Exec and NetBackup systems.

Backup Exec and NetBackup are complex solutions for different types of backups. They use V-Ray technology able to control virtual file systems and applications with further transparent copying and file deduplication which reduces the size of backup copy.

There is also implemented a data deduplication technology in Backup Exec and NetBackup which reduces data duplication and number of physical carriers for storage. Backup solution by Veritas offers three types of deduplication: at client/source side; at server; at device. Its usage accelerates backup copying up to 10 times and reduces backup size up to 95%.

Backup Exec, the most widely spread backup solution, can protect both physical and virtual environments. Its main advantages are: backup copying to any storages and quick creation of instant copies of virtual machines; virtual machines protection; restore after disasters.

NetBackup is a cross-platform backup solution suitable for big data volumes and complex protection of physical and virtual systems, applications and databases in corporate data centres. Typical configuration of NetBackup has three-level architecture: master server; media server; agent. Its main advantages are: centralized management; automated restore; remote tape storage management and additional features enhancing functionality.

Conclusion. Thus, Backup Exec will meet demands of organizations with major information services operating under Windows and with backup processes using several storages. NetBackup is best suited for organizations with heterogeneous infrastructure where information services work under different operating systems and use big data volumes. The backup solutions considered in this paper are a critically important component of organization infrastructure and effective tool of information protection.

Keywords: *data, information protection, backup, restore, informational and technological infrastructure, technology, deduplication, virtual machines.*

Ю.М. Лисецькій, д-р технічних наук, генеральний директор,
ДП «ЭС ЭНД ТИ УКРАИНА»,
Київ, 03680, просп. Академіка Палладіна, 44, Україна,
Iurii.Lysetskyi@snt.ua

С.В. Козаченко, інженер з обслуговування платформ і операційних систем,
ДП «ЭС ЭНД ТИ УКРАИНА»,
Київ, 03680, просп. Академіка Палладіна, 44, Україна,
Saveliy.Kozachenko@snt.ua

РЕЗЕРВНЕ КОПІЮВАННЯ ЯК ІНСТРУМЕНТ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ. Із зростанням об'ємів інформації, що знаходяться на різних носіях, ускладнюється завдання надійності їх зберігання. Один з інструментів захисту інформації — резервне копіювання і створення інформаційних архівів для швидкого доступу до даних.

Основні системи резервного копіювання та їх особливості. Основні виробники сучасних систем резервного копіювання (СРК) — *IBM* з *Tivoli Storage Manager, EMC* з *Neworker* і *Avamar, Veritas* з *Backup Exec* і *NetBackup*.

Backup Exec і NetBackup — комплексні рішення для виконання різних видів резервного копіювання. Працюють на основі технології *V-Ray*, яка здатна контролювати віртуальні файлові системи і додатки, з подальшим виконанням прозорого резервного копіювання та застосуванням технології дедуплікації файлів, що дозволяє скоротити об'єм резервної копії. Також в *Backup Exec* і *NetBackup* реалізовано технологію дедуплікації даних, що усуває їх дублювання та скорочує кількість фізичних носіїв для зберігання.

У СРК компанії *Veritas* реалізовано три способи дедуплікації: на стороні клієнта/джерела; на сервері; на пристрої, а її використання дозволяє прискорити копіювання в 10 разів, а об'єм копій зменшити на 95 відсотків.

Найбільш поширений СРК — *Backup Exec*, здатний захистити як фізичні, так і віртуальні середовища. Його основні переваги: резервне копіювання на будь-які пристрої зберігання та швидке створення моментальних копій віртуальних машин, захист віртуальних машин, відновлення після аварії.

NetBackup — кросплатформне рішення резервного копіювання, здатне працювати з великими об'ємами даних для комплексного захисту фізичних і віртуальних систем, додатків і БД в корпоративних ЦОД. *NetBackup* у своїй типовій конфігурації має трирівневу архітектуру: майстер-сервер, медіа-сервер, агент. Його основні переваги: централізоване управління, автоматизоване аварійне відновлення, управління видаленими стрічковими накопичувачами і додаткові функції, що розширюють функціональність.

Висновки. Таким чином, *Backup Exec* підійде організаціям, в яких основні сервіси працюють під управлінням *Windows* і резервне копіювання виконується на декілька облаштувань зберігання. *NetBackup* краще застосуємо в організаціях з гетерогенною інфраструктурою, де сервіси працюють під різними ОС і з великими об'ємами даних. Розглянуті СРК є критично важливим елементом інфраструктури організації та ефективним інструментом забезпечення захисту інформації.

Ключові слова: *дані, захист інформації, резервне копіювання, відновлення, інформаційно-технологічна інфраструктура, технологія, дедуплікація, віртуальні машини.*