

В.М. Франчук,
кандидат педагогічних наук, доцент,
Національний педагогічний університет імені М.П. Драгоманова

РЕЗЕРВНЕ КОПІЮВАННЯ ДАНИХ

Анотація. У статті розглядаються засоби резервного копіювання даних, як один із способів захисту даних в комп'ютерних системах. Існує кілька технологій резервного копіювання даних: архівація системи, снєпшоти файлових систем, повні копії файлових систем, RAID та перевірка «відбитків файлів». Резервне копіювання даних полягає у збереженні копій програм на носіях: стримерах, оптичних, гнучких та жорстких (внутрішніх чи зовнішніх) магнітних дисках, інших змінних носіях, RAID-масивах, хмарних дисках, тощо. Саме використання хмарних дисків дозволяє швидко та в on-line режимі синхронізувати файли з файлами на персональному комп'ютері та у «хмарі», тому у статті більш детально описано використання та створення резервних копій з використанням хмарних сервісів.

Ключові слова: захист даних, резервне копіювання, хмарні сервіси.

У своїй діяльності підприємства постійно стикаються із завданнями управління існуючими електронними інформаційними ресурсами. До основних питань, які підприємствам необхідно вирішувати в цьому контексті, відносяться: лавиноподібне зростання обсягів даних, що зберігаються, і, як наслідок, необхідність нарощування ємності систем зберігання даних, збільшення обсягів резервного копіювання і часу відновлення, складність управління даними; гарантоване зберігання даних впродовж певного періоду часу, якого вимагають внутрішні політики організації, а також регулюючі органи.

Не лише у великих підприємствах зберігати дані доцільно в архівах і на надійних носіях — магнітних, оптичних, магнітооптичних і т.д. Не тільки системний адміністратор, а й будь-який користувач має вміти використовувати процедури резервного копіювання і архівування даних, а для резервування, довготривалого та гарантованого зберігання даних у домашніх умовах

користуватись змінними жорсткими дисками, пристроями зберігання даних на базі флеш-пам'яті, гібридними накопичувачами тощо [1].

Резервне копіювання (резервування) – копіювання даних з метою подальшого швидкого їх відновлення. Розрізняють: повне резервне копіювання (копіювання всіх файлових систем серверів разом зі всіма системними даними і прикладними завданнями), диференційоване резервне копіювання (лише зміни з моменту останнього повного резервного копіювання), інкрементальне резервне копіювання (зміни з моменту останнього резервного копіювання).

Як свідчить практика, слід створювати резервні копії особистих файлів, програм і системних налаштувань. Також слід створювати контрольні точки відновлення, щоб у разі необхідності мати змогу повернути дані на комп'ютері до попереднього стану.

До найбільш поширених технологій, які використовуються для резервного копіювання, відносяться:

- Архівація системи у повному обсязі з копіюванням на який-небудь надійний зовнішній носій і розміщенням його далеко від основної системи (цей метод вимагає багато часу і незручний в процесі відновлення).
- Снепшоти файлових систем. Використовуються лише для запобігання випадкового вилучення файлів, але якраз в цьому випадку дуже корисні і ефективні.
- Повні копії файлових систем або дисків. Для захисту від відмови жорстких дисків цей спосіб дещо поступається RAID; для відновлення випадково вилучених файлів може бути порівнянний за зручністю зі снеспшотами, залежно від ситуації.
- RAID (англ. Redundant Array of Independent Disks) – технологія віртуалізації даних, за якою об'єднуються кілька дисків в логічний елемент для надійності зберігання даних та підвищення продуктивності накопичувачів. Мінімізуються або виключаються зовсім простої в разі відмови жорстких дисків. Хоч середня частота таких відмов збільшується (оскільки кількість дисків більша), але ліквідувати їх наслідки стає простіше.

- Перевірка «відбитків файлів» (fingerprints). Використання цього методу допомагає з'ясувати, коли потрібно звертатися до резервних копій. Особливо це важливо для «оффлайнових» резервних копій.

Існують і інші стратегії резервного копіювання; більшість з них є композиціями згаданих. Наявність спеціальних вимог, як правило, приводить до спеціалізованих технологій (наприклад, резервне копіювання бази даних, як правило, вимагає використання методів, специфічних для відповідної СУБД). Головним залишається знання небезпек втрати даних, від яких потрібно унебезпечити, і методів захисту від них.

Резервне копіювання, дублювання носіїв є одним з методів захисту даних. Це дозволяє захистити комп'ютерні дані від різного роду непередбачуваних подій – будь-то вірус, фізичне руйнування вінчестера чи викрадання комп'ютера. Резервне копіювання даних полягає у збереженні копій програм на носіях: стримерах, оптичних, гнучких та жорстких (внутрішніх чи зовнішніх) магнітних дисках, інших змінних носіях, RAID-масивах, хмарних дисках, тощо.

У домашніх умовах за необхідності гарантованого зберігання комп'ютерних даних можна встановити другий внутрішній жорсткий диск та використовувати його лише для зберігання резервних копій файлів. Такий диск не буде пошкоджено в разі збоїв у функціонуванні операційної системи. Для резервування даних можна також спеціально відвести окремий комп'ютер і, наприклад, на одному з його жорстких дисків зберігати резервні копії важливих даних. Через USB-порт можна до комп'ютера під'єднувати зовнішні жорсткі диски і відповідно до наперед продуманої політики резервного копіювання зберігати на них важливі файли.

Файли можна зберігати також на CD- чи DVD-дисках. Добре, якщо такі диски будуть записуваними, тобто в разі потреби можна буде змінювати їх вміст – додавати чи вилучати дані. Щоб у подальшому легко можна було знайти потрібний диск, рекомендується в процесі резервування даних позначати диски датою й часом створення.

Якщо комп'ютер під'єднано до мережі, то у разі наявності належних

дозволів для доступу до мережі резервне копіювання можна здійснювати на спеціально відведений мережевий пристрій.

Взагалі, політика резервування – справа суто індивідуальна. Можна резервувати дані щодня, але в будь-якому випадку не рідше одного разу в тиждень. І не записувати дані поверх попередніх, адже ніколи не можна бути впевненим, що нові дані вже не спотворені.

За допомогою більшості сучасних програм резервування можна отримати у тому чи іншому вигляді доступ до бази даних про зарезервовані файли і деякі дані про те, де саме знаходяться останні резервні копії [1].

Одним із сучасних засобів для резервного копіювання є використання хмарних сервісів для зберігання файлів. Найбільш популярними і доступними для закладів вищої освіти є хмаро-орієнтовані сервіси Office 365 для навчальних закладів та Google Apps для навчальних закладів.

У Office 365 для навчальних закладів для резервного копіювання можна використовувати сервіс OneDrive. OneDrive (раніше – SkyDrive, Windows Live SkyDrive і Windows Live Folders) – це файловий хостинг, що надається компанією Microsoft як частина набору онлайн-послуг. За допомогою OneDrive користувачі можуть зберігати файли, а також інші особисті дані, такі як налаштування операційної системи Windows у «хмарі». Файли можна синхронізувати з файлами, які зберігаються на комп'ютері користувача та отримувати доступ до них з веб-браузера або мобільного пристрою, а також ділитися публічно або з певними користувачами. У сервісі OneDrive пропонується 5 Гбайт вільного місця для зберігання даних. Додатковий обсяг пам'яті можна додати окремо або через підписку на інші служби Microsoft, включаючи Office 365, зокрема для користувачів Office 365 для навчальних закладів виокремлюється дисковий простір до 1 Тбайта (Рис. 1).

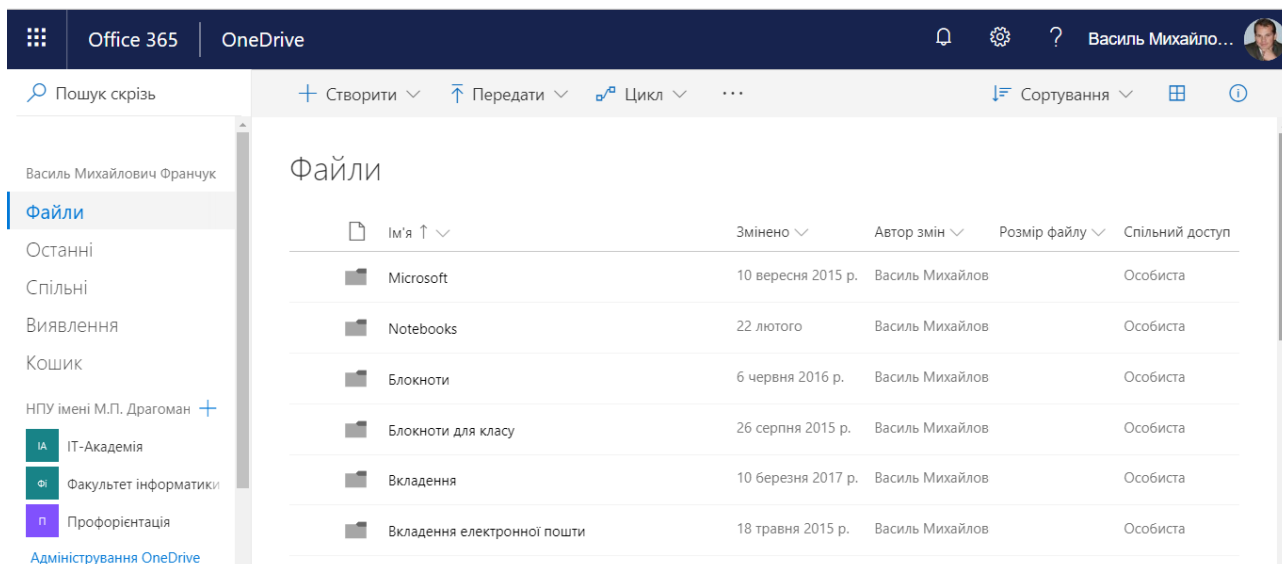


Рис. 1.

Компанія Microsoft також випустила клієнтські програми OneDrive для Android, iOS, Windows 8, Windows 10, Windows 10 Mobile, Windows Phone Xbox 360, і Xbox One, використання яких дозволяє користувачам переглядати та впорядковувати файли, що зберігаються в хмарному сховищі OneDrive. Крім того, Microsoft випустила додатки для Microsoft Windows, використання яких дозволяє користувачам синхронізувати весь обсяг OneDrive з їх комп'ютерами для автономного доступу, а також між кількома комп'ютерами. Використання клієнтської програми OneDrive для Windows дозволяє користувачам завантажувати (синхронізувати) файли, які зберігаються на персональному комп'ютері користувача (Рис. 2). Використання версій для операційних систем Android, iOS та Windows Phone 8 також дозволяють автоматично завантажувати фотографії з камери на OneDrive.

Окрім клієнтських додатків, OneDrive інтегрований в операційну систему Windows (починаючи з версії 8.1), використання якого надає користувачам доступ до документів, фотографій та відеозаписів, які зберігаються в їхніх облікових записах OneDrive. Також за допомогою OneDrive у Windows 8.1 можна синхронізувати налаштування та файли користувача.

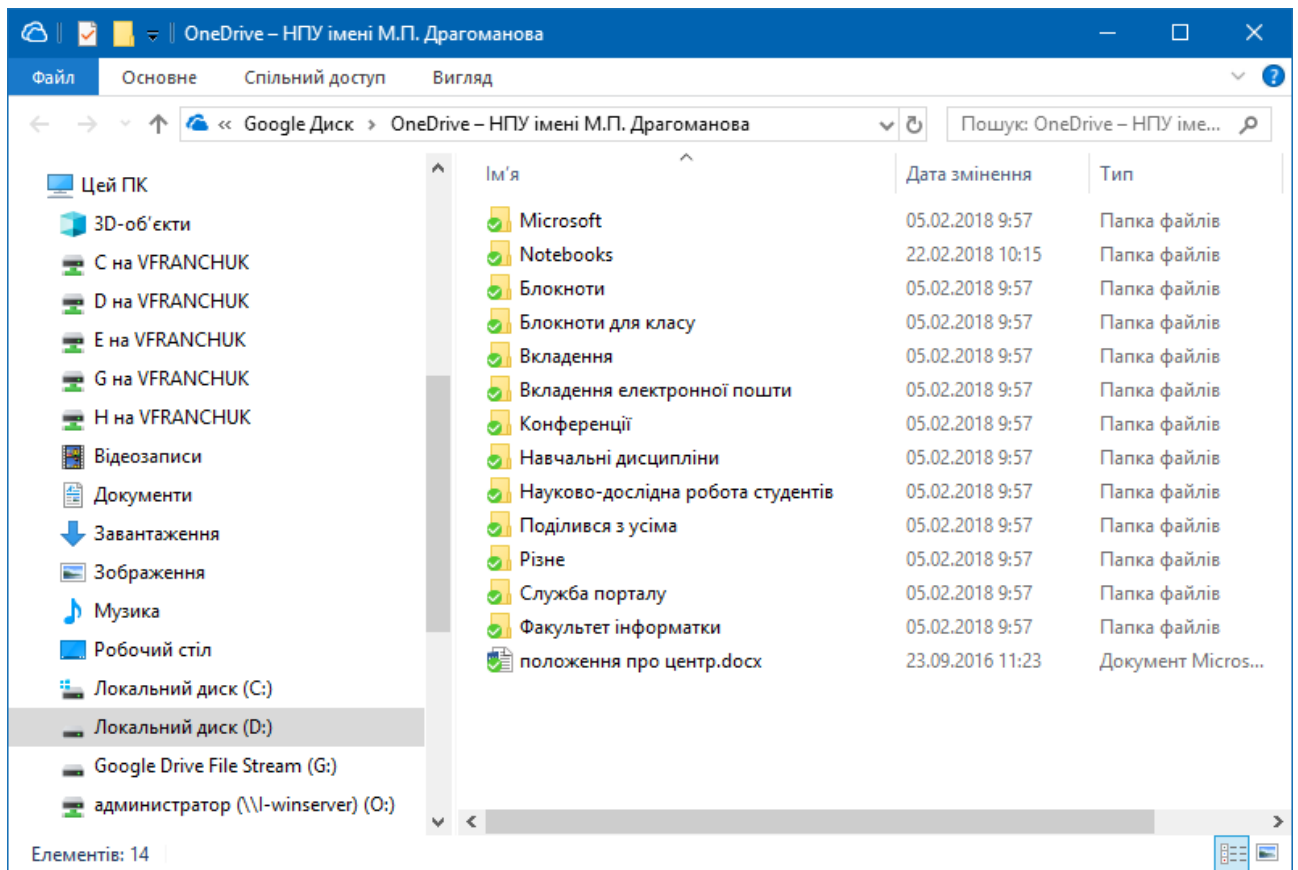


Рис. 2

Користувачі останніх версій Microsoft Office (починаючи з MS Office 2010) можуть використовувати прикладні програми для одночасного редагування документів, що зберігаються на OneDrive. Зміни синхронізуються, коли користувачі зберігають документ, і коли виникають конфлікти, користувач, який зберігає дані, може вибрати, яку саме версію зберегти. Користувачі можуть також використовувати кілька різних прикладних та веб-програм для редагування того самого документа. Починаючи з Office 2016, інтеграція OneDrive може бути відключена в налаштуваннях програми OneDrive.

Користувачі Microsoft OneNote можуть синхронізувати один або кілька своїх Class Notebook (Class Notebook – це OneNote для персоналу навчальних закладів) за допомогою OneDrive. Коли Class Notebook вибирається для спільного використання, на OneDrive створюється копія Class Notebook з комп'ютера користувача на OneDrive, і ця онлайн-копія стає оригіналом для всіх майбутніх змін [3].

Ще одним із сучасних засобів для резервного копіювання з використанням

хмарних сервісів для зберігання файлів є сервіс Google Drive від компанії Google.

Google Drive включає в себе систему обміну файлами, де автор файлу або папки за замовчуванням є його власником. Власник має можливість надавати доступ до файлу або папки для інших користувачів. Право власності може передаватися іншим користувачам. Файли і папки можуть спільно використовуватись приватно конкретними користувачами, які мають обліковий запис Google, використовуючи свої @gmail.com адреси електронної пошти або корпоративної пошти, зареєстрованої у Google. Для спільного використання файлів з користувачами, які не мають облікового запису Google, потрібно зробити файли «Доступний за посиланням». Це створює секретний URL для файлу, який може бути відкритий з використанням електронної пошти, блогу і т. д. Файли та папки можна також зробити «Загальнодоступними в Інтернет», це означає, що вміст файлу може бути проіндексований пошуковими системами і, таким чином, може бути знайдений і доступний будь-кому (Рис. 3). Власник може також встановити рівень доступу. Є три запропоновані рівні доступу – «Може редагувати», «Може коментувати» і «Може переглядати». Користувачі, яким надається доступ для редагування, можуть запрошувати інших редагувати [2].

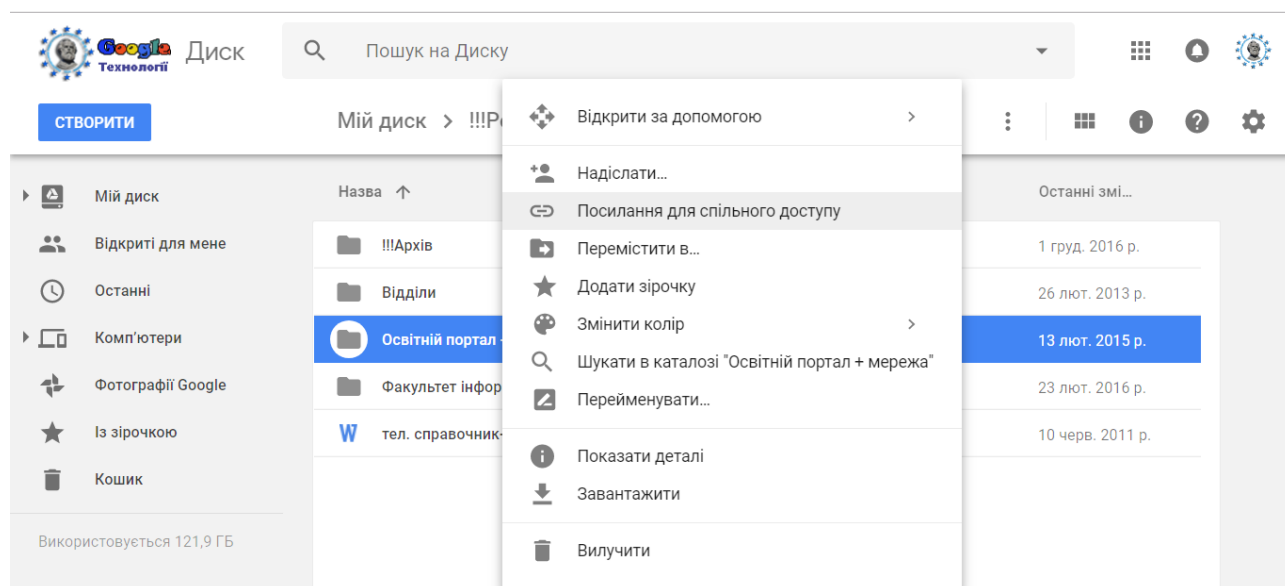


Рис. 3

Для синхронізації та резервного копіювання файлів у Google розробили два програмних засоби: «Клієнт Google Диску» та «Резервне копіювання і

синхронізація».

За допомогою «Клієнта Google Диску» можна шукати і переглядати файли з Google Диску на комп'ютері, а також:

- Зберігати файли і папки (в тому числі на загальних дисках) для роботи в офлайн-режимі.
- Переглядати і систематизувати об'єкти, використовуючи файлову систему комп'ютера.
- Відкривати файли в додатках, встановлених на комп'ютері.
- Переглядати всі файли на Google Диску, не використовуючи дисковий простір на комп'ютері (Рис. 4).

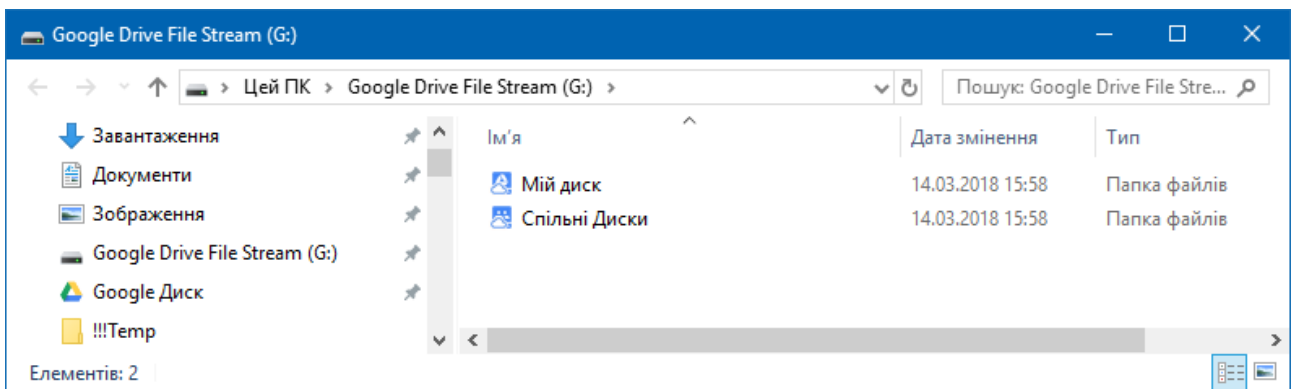


Рис. 4

За допомогою програмного засобу «Резервне копіювання та синхронізація» можна синхронізувати файли між комп'ютером і Google Диском, а також вибрати файли для резервного копіювання з комп'ютера користувача на Google Диск (Рис. 5).

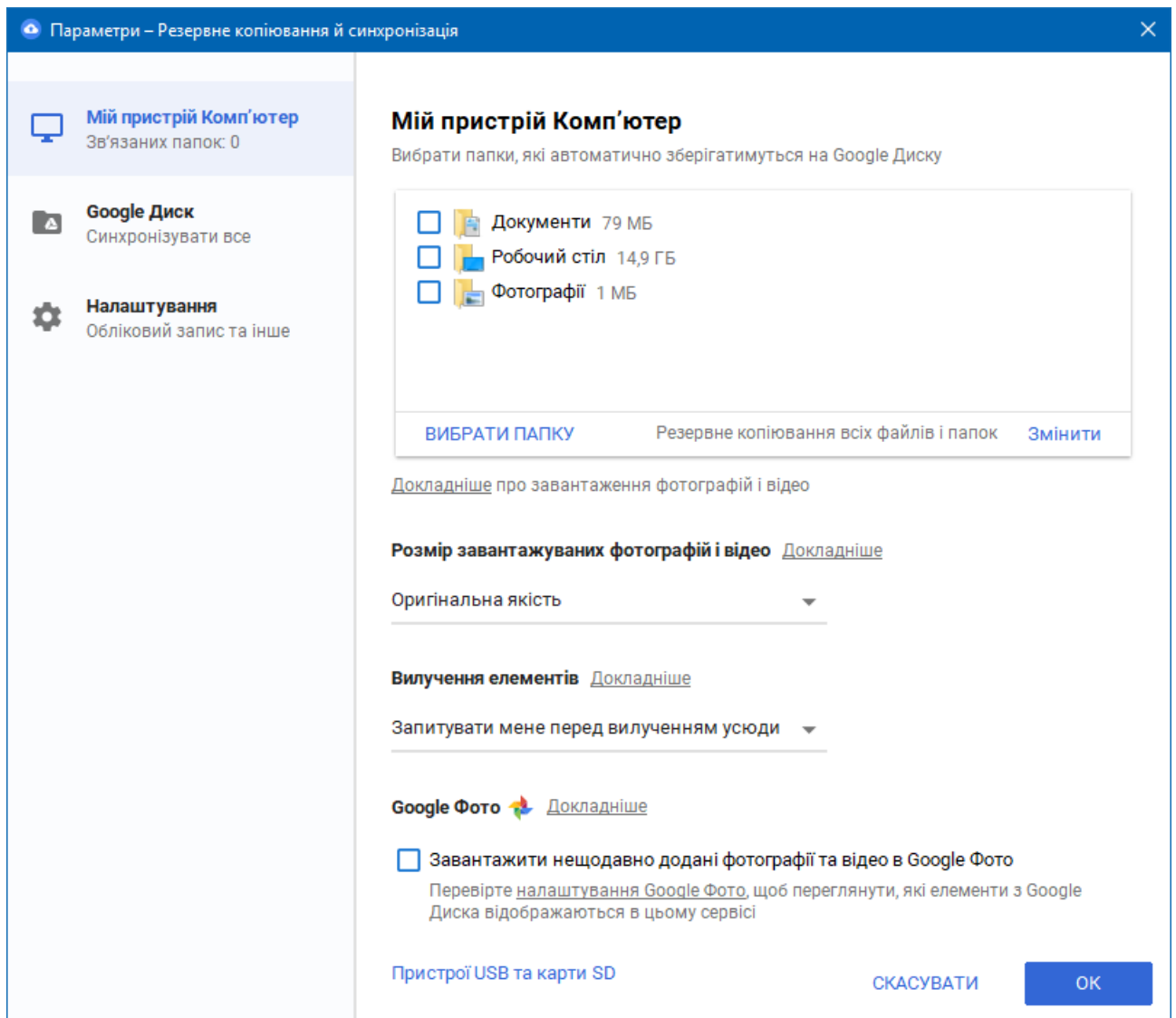


Рис. 5

Основні характеристики програмних засобів від Google «Резервне копіювання і синхронізація» та «Клієнт Google Диску» наведено у таблиці №1.

Таблиця №1.

Характеристики Програмні засоби	Резервне копіювання і синхронізація	Клієнт Google Диску
Використання файлів в розділі «Мій диск».	Так	Так
Використання файлів на загальних дисках.	немає	Так
Синхронізація вибраних папок в розділі «Мій диск».	Так	Так
Синхронізація окремих файлів в розділі.	немає	Так

«Мій диск»		
Робота з прикладними програмами, такими як Microsoft Office або Adobe Photoshop.	Так	Так
Синхронізація інших папок, наприклад «Документи» або «Робочий стіл».	Так	немає
Робота в обліковому записі Google	Так	немає

Отже, основними перевагами використання хмарних сервісів для зберігання даних є: 1) захист від несанкціонованого доступу; 2) необмежений обсяг для зберігання даних; 3) захист від втрати даних; 4) доступність з різних пристроїв (комп'ютер, планшет, телефон тощо).

В процесі використання хмарних сервісів для зберігання даних є можливість: 1) синхронізувати файли, тобто в разі зберігання файлу в хмарному середовищі можна отримати доступ до цього файлу з будь-якого пристрою, з якого є вихід в глобальну мережу Інтернет; 2) робити резервні копії файлів, для уникнення їх втрати можна надсилати дані на віддалений комп'ютер; 3) працювати з файлом колективно, тобто є можливість надати дозвіл на перегляд та редагування файлу кільком користувачам.

Ідеального захисту даних немає. Але все-таки слід зазначити, що, скориставшись перерахованими вище способами, можна досягти досить високого ступеня захищеності даних на персональному комп'ютері.

Список використаних джерел

1. Смалько О.А. Захист інформаційних ресурсів: Монографія. - Кам'янець-Подільський: ПП Буйницький О А, 2011. - 704 с.
2. Google Drive. Режим доступу: https://uk.wikipedia.org/wiki/Google_Drive.
3. OneDrive. Режим доступу: <https://uk.wikipedia.org/wiki/OneDrive>.

В.М. Франчук

РЕЗЕРВНОЕ КОПИРОВАНИЯ ДАННЫХ

Аннотация. В статье рассматриваются средства резервного копирования данных, как один из способов защиты данных в компьютерных системах. Существует несколько технологий резервного копирования данных: архивация системы, снэпшот файловых систем, полные копии файловых систем, RAID и проверка «отпечатков файлов». Резервное копирование данных заключается в сохранении копий программ на носителях: стримерах, оптических, гибких и жестких (внутренних или внешних) магнитных дисках, других сменных носителях, RAID-массивах, облачных дисках и т.п. Именно использование облачных дисков позволяет быстро и в on-line режиме синхронизировать файлы с файлами на персональном компьютере и в «облаке», поэтому в статье более подробно описано использование и создание резервных копий с использованием облачных сервисов.

Ключевые слова: защита данных, резервное копирование, облачные сервисы.

V.M. Franchuk

DATA BACKUP

Resume. The article discusses backup data as one of the ways to protect data in computer systems. There are several data backup technologies: system archiving, file system snapshots, full file system files, RAID, and file-checking. Backing up data is to keep copies of programs on media: tape drives, optical, flexible and hard (internal or external) magnetic disks, other removable media, RAID arrays, cloud drives, and more. The use of cloud drives makes it possible to quickly and in-line synchronize files with files on a personal computer and in a "cloud", so the article describes in more detail the use and creation of backups using cloud services.

Keywords: data protection, backup, cloud services.