УДК 004.25.58(043)

*І.А. Прохіцький*
*(Національний авіаційний університет, Україна)*

**Захист інформації при використанні хмарних сховищ**

*В роботі розглядаються поняття «хмарні технології», які здатні задовольняти потреби у віддаленій обробці даних. Хмарні сервіси дають можливості постійного доступу до віддалених інтернет-ресурсів. Важлива роль у процесі його використання питання захисту інформації, тому названі деякі правила, дотримання яких забезпечить захист даних при користуванні сховищами.*

Хмарні обчислення являється моделлю, що надає зручний доступ до спільного використання обчислювальних ресурсів через мережу, їх можна налаштувати, і вони можуть бути швидко надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера.

Хмарні технології можна вважати «розподіленими технологіями». Це означає, що для опрацювання даних використовується не один стаціонарний комп'ютер. Для цього усі задачі розподіляються по комп'ютерах, які мають підключення до мережі. Хмарні технології являють собою інформаційно-комунікаційні технології, які передбачають можливість віддаленого опрацювання та зберігання даних. Як показує практика, найбільш доречно його застосовувати з метою захисту файлів, а також для збереження пам'яті на різних пристроях [4, с. 44].

За сучасних умов хмарні технології являють собою одну велику концепцію, яка складається з великої кількості різних понять. Його складовими елементами є: програмне забезпечення, інфраструктура, платформа, дані, робоче місце і т.д. Хмарні технології виконують надзвичайно важливу функцію – це задоволення потреб користувачів, яким необхідною є віддалена обробка даних.

Сервіси, які надають користувачам можливість постійного доступу до віддалених інтернет-ресурсів (серверів, додатків, сховищ тощо), називаються «хмарними сервісами».

Хмарне сховище даних являє собою модель онлайн-сховища, у якому дані можуть зберігатися на серверах, які розподілені в мережі, які надаються в користування клієнтам третьою стороною-постачальником. Зберігання та обробка даних відбувається в так званій «хмарі», яка являє собою, з точки зору клієнта, один великий віртуальний сервер. Якщо брати до уваги їх фізичне розташування, то такі сервери можуть знаходитися на великій відстані один від одного. Постачальники хмарних систем зберігання даних відповідають за зберігання наявної інформації і доступ до неї, а також за роботу фізичного середовища. Користувачі купують у постачальників послуг хмарного сховища змогу зберігати там дані. У результаті використання віртуальних сховищ користувачі отримують широкі можливості. Зокрема, вони мають можливість отримати доступ до файлів з будь-якого пристрою (комп'ютера, планшета, телефону) і з будь-якої точки світу, в якій є підключення до мережі інтернет. Також можна автоматично робити резервні копії даних у хмару, що зменшує ймовірність їхньої втрати у

випадку, якщо станеться збій або жорсткий диск вийде з ладу. Існує можливість налагодження максимального захисту інформації від вірусів та несанкціонованого доступу.

Хмарне сховище відкриває перед своїми користувачами можливість доступу до усіх даних не залежно від того, у якій точці земної кулі знаходяться користувачі. При цьому вони можуть використовувати для цього будь-які доступні для них пристрої. І це є надзвичайно важливою перевагою. Проте це відкриває також широкі можливості для кіберзлочинців, які можуть отримати доступ до чужих файлів. Саме через існування такої загрози значна кількість людей турбуються про свою безпеку у сховищі, тому шукають додатковий рівень безпеки. Отже, ключовим питанням залишається безпека файлів та документів, які зберігаються на таких сервісах.

Існують деякі правила, дотримання яких забезпечить захист даних, які розміщені у хмарному сховищі.

В першу чергу вважаємо за необхідне зупинитися на безпеці профілю. Як показує практика, переважна частина людей, які користуються мережею, захищають свої акаунти у різних облікових записах, використовуючи для цього лише паролі. Проте такий метод не є надійним. Велика частина людей, які користуються паролями, допускають одну важливу помилку. Вона полягає у використанні комбінацій цифр під час створення своїх паролів («12345», «123456», «12356789»). Для кіберзлочинців немає жодних труднощів у тому, щоб розгадати такі паролі. Також до найбільш популярних помилок, які допускають користувачі, належить повторне використання паролів, що збільшує ризики стати жертвою атак шляхом заповнення облікових даних. Через це виникає необхідність у забезпеченні додаткового рівня безпеки за допомогою двофакторної аутентифікації не лише для хмарних сховищ, а й інших облікових записів. Вона передбачає використання 3 основних факторів аутентифікації: те, що знає користувач (пароль або PIN-код), те, що має користувач (фізичний ключ або токен безпеки), те, якими є користувач (відбиток пальця або сканування сітківки ока). Частіше за все для того, щоб у війти в систему, використовуються два з цих факторів. У такому випадку навіть якщо кіберзлочинці будуть мати пароль до деякого профілю, вони не матимуть змоги отримати доступ до нього, не маючи додаткового фактору [3].

Серед багатьох користувачів набирають все більшої популярності сторонні додатки, так як вони спрощують завдання, які стоять перед користувачами, а також допомагають в ефективному налагодженні роботи. Проте варто пам’ятати при цьому про безпеку роботи та про захист даних. Існує велика кількість додатків, які здатні підвищити продуктивність користувачів. Проте, використовуючи додатки сторонніх розробників, варто бути особливо обережними та робити перевірку кожної програми перед тим, як її встановлювати. Ознайомившись з відгуками та оцінками програми, необхідно поцікавитися політикою конфіденційності постачальника, умовами обслуговування та політикою видалення.

Питання безпеки усіх хмарних сховищ постійно вдосконалюються, проте, не зважаючи на це, виникають інциденти, які пов’язані з витоками даних. Частіше за все причиною цього є людські помилки або атаки кіберзлочинців.

Не зважаючи на те, що дані користувачів в різних G Suite чи інших сервісах є зашифрованими як при передачі, так і при зберіганні, для того, щоб забезпечити підвищення безпеки, необхідно використовувати шифрування файлів перед тим, як завантажувати їх у хмару. У такому випадку навіть якщо кіберзлочинці отримають доступ до даних сховища, то вони не зможуть переглянути дані без наявності ключа дешифрування [2, с. 91].

Раніше ми розглядали те, що сховище, як наприклад «Google Диск» може використовуватися для того, щоб завантажувати та зберігати файли, а також існує можливість обміну та навіть спільної роботи над документами з іншими користувачами. Для цього достатньо поділитися посиланням з конкретною людиною зручним способом. Також можна надати права читача чи редактора. Користувач, який матиме права читача, зможе переглядати файли, які знаходяться в папці, а права редактора надають йому можливість створення, додавання та редагування документів. У такому випадку необхідно бути досить уважними та звертати увагу на те, яким користувачам надається дозвіл на використання спільних документів. Для того, щоб заблокувати можливість спільного використання файлу або папок у деякого користувача, достатньо лише видалити його ім'я зі списку. Також можна обмежити загальний доступ до файлів та заборонити користувачам можливість завантаження, копіювання або їх друк.

**Висновки:** Отже, для багатьох людей використання хмарних сховищ є досить популярним та зручним способом доступу до даних. Google Drive є безумовним лідером серед багатьох відомих на сьогоднішній день мережевих сховищ даних. Він містить багато переваг та ним зручно користуватися. Проте застосування будь-якого хмарного середовища для зберігання даних є гарним варіантом за умови, якщо будуть дотримані основні правила безпеки. Зокрема, необхідно бути обережним з користувачами, який надається дозвіл користування файлами, а також з налаштуваннями часу, протягом якого можуть бути поширені документи, застосовувати шифрування даних. Крім цього, рекомендують здійснювати регулярну перевірку вмісту Google Диску та слідкувати за його безпекою так само, як і за іншими хмарними сервісами.

## Список літератури


1. Биков В. Ю. Технології хмарних обчислень, ІКТ-аутсорсінг та нові функції ІКТ підрозділів навчальних закладів і наукових установ. *Інформаційні технології в освіті*. Херсон, 2011. № 10. С. 8–23.
2. Захист інформаційних ресурсів: навчально-методичний посібник до курсу «Захист інформаційних ресурсів» / укл. С. О. Троян. Умань, 2012. 120 с.
3. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навчальний посібник. Харків : Вид. ХНЕУ, 2013. 476 с.
4. Смірнова Т. В., Поліщук Л. І., Смірнов О. А. Дослідження хмарних технологій як сервісів. 2020. № 7(3). С. 43–62.
5. Віблий В.М., Смотр О.О. Безпека інформації у хмарних сховищах. Збірник тез доповідей ІІІ м. Львів, 28 листопада 2019 року. Львів, 2019. С. 88–90.