

АНАЛІЗ БЕЗПЕКИ СЕРВІСІВ ЗБЕРІГАННЯ ДАНИХ У ХМАРІ

К.А. ПОГРЕБНЯК, Д.В. ПОВТАРЄВ

Стаття присвячена аналізу сервісів зберігання інформації у хмарі. Для аналізу сервісів визначаються критерії безпеки, за якими проводиться порівняння. Розглядаються такі сервіси: Dropbox, SkyDrive, GoogleDrive, Wuala та Yandex.Disk. Основна увага приділяється аналізу інтерактивного входу в систему, реєстрації, формуванню захищеного каналу зв'язку та механізмам безпеки зберігання даних.

Ключові слова: хмарні обчислення, сервіс зберігання інформації, безпека зберігання даних.

ВСТУП

За останні роки кількість сервісів зберігання даних, що ґрунтуються на публічних хмарах, помітно збільшилась. Зростання попиту користувачів на такі сервіси обумовлено зручністю користування інформацією, зокрема доступу до неї будь-де та будь-коли. Однак, з іншого боку, зручність користування інформацією досягається за рахунок переміщення її на фізичні носії провайдера, що вимагає певних гарантій безпечного зберігання даних та їх функціонування в інформаційних мережах [1]. Зазначимо, що наразі не існує міжнародних стандартів та технічних специфікацій, які визначали б безпечні протоколи передачі та зберігання даних. Тому, на даному етапі розвитку таких сервісів фактично кожен провайдер пропонує свої рішення з забезпечення безпеки інформації. Це призводить до того, що кінцевий користувач повинен самостійно оцінювати якість послуг з точки зору захисту його особистих даних. Тому **актуальною задачею** є аналіз існуючих широко поширених сервісів зі зберігання інформації в публічній хмарі з точки зору безпеки інформації.

1. ОГЛЯД СЕРВІСІВ ЗБЕРІГАННЯ ДАНИХ

Системою зберігання даних у хмарі вважається мережа розподілених центрів обробки даних, які надаються користувачеві третьою стороною та сприймаються ним як один єдиний віртуальний сервер. Для підвищення доступності даних інформація може додатково зберігатися в різних місцях, а деталі реалізації не відомі користувачеві. Користування системою зберігання даних надається у вигляді Інтернет-сервісу [2].

Проаналізувавши наявні сервіси зберігання інформації можна виділити такі популярні в Україні та світі сервіси: Dropbox, SkyDrive, SugarSync, GoogleDrive, Mozy, CrashPlan, Insync, LogMeInCubby, Bitcasa, Strongspace, DollyDrive, SpiderOak, Wuala, Yandex.Disk, Box.net, Amazon-CloudDrive, JungleDisk, GooglePlayMusic, MediaFire, Office365, Zoho, RapidShare, Sendspace, YouSendIt, Carbonite, Flickr, Photobucket, SmugMug, GoogleMusic, AppleiCloud, AmazonCloudPlayer.

Для написання роботи були відібрані такі сервіси: Dropbox, SkyDrive, GoogleDrive, Wuala, Yandex.Disk.

Стислий опис кожного з них та пояснення причин відбору наведені нижче.

Dropbox управляється DropboxInc, яка знаходиться в Сан-Франциско, США. Dropbox був обраний, оскільки він є одним з найпопулярніших у світі провайдерів хмарного зберігання даних. Він отримав широке висвітлення в засобах масової інформації і цілком може становити суть того, як хмарні сервіси зберігання бачать сьогодні. Сервіс дуже простий в установці, зручний у використанні і доступний безкоштовно або за низьку ціну. Він був розроблений як самостійний хмарний сервіс зберігання даних і забезпечує обмежену інтеграцію в популярних операційних системах.

Wuala існує з 2007 року і працює з березня 2009 року як власність компанії LaCie AG111, яка знаходиться в Цюриху.

До переліку обраних сервісів Wuala потрапив через те, що він реалізує максимальний набір функцій, поширених серед хмарних сервісів та позиціонується як такий, що забезпечує високий криптографічний рівень захисту даних. Крім того, цей сервіс має одну з найвищих швидкостей взаємодії, та монтується як диск з кешуванням – це може потенційно привабити велику кількість користувачів.

Yandex.Disk належить російській компанії Яндекс та знаходиться на ринку з 2012 року. Яндекс є найбільшою Інтернет компанією на пострадянському просторі. Пошукова система Яндекс посідає друге місце в Україні станом на березень 2013 року, займаючи майже 30% ринку (за даними liveinternet.ru). Виходячи з цього факту, можна зробити висновок, що велика частина користувачів обере послуги цього сервісу.

MicrosoftSkyDrive (скорочено – SkyDrive) створений у серпні 2007 року і керується компанією Microsoft. Сервіс є частиною набору онлайн послуг Windows Live. Microsoft є найбільшою світовою компанією з розробки програмного забезпечення. Великий ступінь інтеграції різноманітного програмного забезпечення (в тому числі iMicrosoft SkyDrive), з сімейством найпопулярніших операційних систем сучасності безумовно

забезпечить гідний рівень використання цього сервісу серед користувачів та організацій.

GoogleDrive є хмарним сховищем даних, створеним в 2012 році компанією GoogleInc. GoogleDrive замінює собою GoogleDocs після активації. Поширеність додатків Google, високий рівень використання GoogleDocs та очікувань від його наступника є передумовами включення цього сервісу до списку.

В цій роботі проводиться порівняння найбільш популярних сервісів за методологією, що наведена в [3].

Кожний сервіс включає в себе частини як клієнтського, так і серверного програмного забезпечення. Відповідно до підходу аналізу, пропонується розглянути виключно клієнтську частину програмного забезпечення.

Для реалізації високого рівня безпеки сервіси повинні забезпечувати високий рівень як мінімум наступних аспектів безпеки, які можуть суттєво впливати на рівень захищеності інформації, що зберігається:

1) вхід у систему та реєстрація, для захисту від викриття та збору інформації та з метою примусового використання надійних паролів;

2) використання захищеного каналу для забезпечення транспортної безпеки між клієнтом і сервером;

3) безпека зберігання даних для унеможливлення вивчення даних постачальником послуг.

Існують інші характеристики, які потенційно можуть вплинути на рівень безпеки даних. До них відносяться безпечний обмін файлами, що зберігаються, дедуплікація, безпечне використання декількох пристроїв для доступу, функції оновлення програмного забезпечення тощо. Аналіз цих характеристик не входив до задач цієї роботи і буде виконаний у подальшому.

2. АНАЛІЗ СЕРВІСІВ ЗБЕРІГАННЯ ДАНИХ

Для аналізу сервісів визначимо критерії та показники, за якими проводитиметься порівняння:

- Вхід у систему та реєстрація
 - обмеження на довжину пароля;
 - захист від атаки перебору пароля;
 - двофакторна автентифікація;
 - механізм відновлення пароля.
- Захищений канал зв'язку:
 - протокол формування захищеного каналу зв'язку;
 - алгоритм автентифікації повідомлень;
 - алгоритм узгодження ключів.
- Безпека зберігання даних
 - алгоритм шифрування даних;
 - володіння ключем шифрування даних.

Послідовно проаналізуємо кожний з сервісів нашого списку відносно наведених критеріїв безпеки.

2.1 Аналіз сервісу зберігання даних Dropbox

2.1.1 Вхід у систему та реєстрація

Для реєстрації і входу в систему використовується захищений канал зв'язку (TLS).

Реєстрація може бути здійснена на веб-сайті або під час установки клієнта.

Під час реєстрації на веб-сайті користувач повинен ввести ім'я та прізвище (довільні рядки), адресу електронної пошти та пароль. Одна адреса електронної пошти може бути пов'язана тільки з одним обліковим записом.

Під час реєстрації накладаються обмеження на мінімальну довжину пароля, яка має бути не менше за шість символів, максимальне обмеження не встановлене. Крім того як пароль не повинна використовуватися адреса електронної пошти.

При реєстрації на веб-сторінці Dropbox надає підказку про якість обраного пароля, проте приймає слабкі паролі.

Процес реєстрації під час установки клієнта трохи відрізняється: клієнтський додаток не має індикатора надійності пароля і користувач повинен повторити пароль. При введенні адреси, що вже була використана, відображується відповідне повідомлення. При першому вході через клієнтський додаток користувач вводить адресу електронної пошти та пароль. Після проходження перевірки автентичності маркер безпеки передається на сервер і зберігається на клієнтській частині для подальшої автентифікації користувача.

Dropbox не відправляє активаційного повідомлення на електронну пошту відразу після реєстрації, це відбувається лише після спроби отримати перший URL для загального доступу до файла, тож користувач може використовувати новий обліковий запис одразу після заповнення реєстраційної форми.

У разі невдалої спроби входу в систему, Dropbox повідомляє користувача, що один елемент з пари логін/пароль є неправильним, проте не уточнює який саме.

Якщо користувач втратив свій пароль, Dropbox відправляє повідомлення на зареєстровану електронну пошту користувача. Цей лист містить URL захищеної веб-сторінки для введення нового пароля.

Dropbox запобігає перебору паролів, тимчасово блокуючи обліковий запис після багатьох невдалих спроб входу в заданий період часу.

Dropbox має можливість використання двофакторної автентифікації. Ця опція може бути ввімкнена в налаштуваннях профілю. Використовуються одноразові коди доступу, які можна отримувати на мобільний телефон. Крім того є можливість використовувати баркоди за допомогою TimeBasedOneTimePassword мобільних додатків.

Результати аналізу сервісу Dropbox за критерієм «Вхід у систему та реєстрація» наведено в таблиці 1.

Таблиця 1

«Вхід у систему та реєстрація» для сервісу Dropbox

Мінімальна довжина пароля	6 символів
Захист від атаки перебору пароля	Тимчасове блокування
Двофакторна автентифікація	Пароль та одноразовий код доступу, що передається на мобільний телефон чи за допомогою використання баркодів
Механізм відновлення пароля	Надсилається URL сторінки, на якій користувач може змінити пароль

2.1.2 Захищений канал зв'язку

В ході аналізу сервісу Dropbox був розглянутий принцип забезпечення захищеного каналу зв'язку між клієнтом та сервером, результати якого наведено у таблиці 2.

Таблиця 2

«Захищений канал зв'язку» для сервісу Dropbox

Протокол формування захищеного каналу зв'язку	TLS 1.1
Алгоритм автентифікації повідомлень	AES_256_CBC (SHA1)
Алгоритм узгодження ключів	ECDHE_RSA (2048 bit)

2.1.3 Безпека зберігання даних

Dropbox використовує AES-256 для шифрування даних, що зберігаються на серверах. Ці дані не будуть зашифровані на стороні клієнта, замість цього Dropbox шифрує дані після завантаження на стороні сервера, використовуючи свій власний ключ шифрування. Оскільки Dropbox шифрує дані на стороні сервера, користувач не може бути впевнений в конфіденційності даних. Результати аналізу за критерієм «Безпека зберігання даних» наведено в таблиці 3.

Таблиця 3

«Безпека зберігання даних» для сервісу Dropbox

Алгоритм шифрування даних	AES-256
Володіння ключем шифрування даних	Ключем володіє провайдер

2.2 Аналіз сервісу зберігання даних Wuala

2.2.1 Вхід у систему та реєстрація

Для реєстрації і входу в систему використовується безпечний канал зв'язку.

Нові облікові записи можуть бути створені тільки за допомогою додатка Wuala.

Під час реєстрації користувач повинен надати унікальне ім'я, адресу електронної пошти та пароль. Одна адреса електронної пошти може бути пов'язана з кількома обліковими записами.

На пароль накладаються лише обмеження на мінімальну довжину, яка повинна бути як мінімум шість символів, максимальне обмеження не встановлено.

Wuala надає підказку про якість обраного пароля під час реєстрації, проте не відкидає слабкі паролі.

Wuala не відправляє активаційного повідомлення на електронну пошту для підтвердження факту реєстрації.

У разі невдалої спроби входу в систему, Wuala повідомляє користувача, що один чи обидва елементи з пари логін/пароль є неправильним, проте не уточнює який саме.

Паролі не зберігаються на серверах Wuala, тому можливість відновлення втраченого пароля відсутня. Wuala забезпечує опційну функціональність підказки пароля. Підказка пароля може бути використана для одного імені користувача або для адреси електронної пошти. Якщо є кілька облікових записів, зареєстрованих за однією адресою електронної пошти – кілька листів буде відправлено, по одному для кожного облікового запису, який має підказку для пароля. Функція підказки пароля дозволяє збір інформації про вже зареєстровані імена користувачів і адреси електронної пошти.

Обмежень на кількість невдалих спроб входу немає.

У Wuala наразі не реалізовано механізм двофакторної автентифікації.

Результати аналізу сервісу Wuala за критерієм «Вхід у систему та реєстрація» наведено в таблиці 4.

Таблиця 4

«Вхід у систему та реєстрація» для сервісу Wuala

Мінімальна довжина пароля	6 символів
Захист від атаки перебору пароля	Відсутній
Двофакторна автентифікація	Відсутня
Механізм відновлення пароля	Відсутній

2.2.2 Захищений канал зв'язку

Wuala використовує власний протокол зв'язку між клієнтом і сервером, а не стандартизовані і добре відомий SSL / TLS. Відповідно до прес-релізів Wuala, використовується перевірка цілісності для захисту даних при передачі, але жодної детальної документації про механізми і протоколи не було опубліковано.

У поєднанні з конвергентними схемами шифрування, що їх використовує Wuala, відсутність шифрування при передачі дозволяє зловмисникам отримати повідомлення, які передаються, і спробувати реалізувати атаки зі збором інформації.

В ході аналізу сервісу Wuala був розглянутий принцип забезпечення захищеного каналу зв'язку між клієнтом та сервером, результати наведено у таблиці 5.

Таблиця 5

«Захищений канал зв'язку» для сервісу Wuala

Протокол формування захищеного каналу зв'язку	Відсутній
Алгоритм автентифікації повідомлень	AES_256 (SHA1)
Алгоритм узгодження ключів	DHE_RSA (2048 bit)

2.2.3 Безпека зберігання даних

Ідея, на якій базуються схеми шифрування Wuala, полягає в наявності ненадійної файлової системи, безпека якої забезпечується криптографічними методами. Використані схеми є реалізацією структури дерева каталогів для криптографічних файлових систем, яка називається Scurtree, що була опублікована в [4]. Довіра ґрунтується на симетричному кореневому ключі, який отримується з пароля користувача. Wuala обчислює окремі ключі для кожного каталогу і окремі ключі для кожного файлу. Всі вони виводяться через кореневий ключ. Вони можуть бути надані партнерам з метою обміну даними.

Wuala використовує конвергентні схеми шифрування [5]. Це означає, що ключ для шифрування файлу є похідним від його геш-значення.

Найбільш важливими властивостями конвергентних схем шифрування є:

1) ідентичні відкриті тексти зашифровуються в ідентичні криптотексти, незалежно від користувача;

2) сервер не може розшифрувати криптотексти, не маючи копію відкритого тексту.

Перша властивість забезпечує реалізацію функції дедуплікації зашифрованих даних. Друга властивість захищає документи, які є унікальними для користувача, наприклад, власноруч написані твори, неопубліковані технічні звіти тощо. З іншого боку конвергентні схеми шифрування мають важливі недоліки, зокрема існує можливість атак у разі, якщо зломисник має доступ до серверної сторони.

Згідно з прес-релізами відзначається, що Wuala використовує AES-256 для шифрування метаданих і інформації, що зберігається. Клієнт підписує кожен файл за допомогою пари ключів користувача, з метою виявлення файлів, які були отримані від сторонніх осіб. Підписи створюються і перевіряються за допомогою RSA-2048, в той час як для перевірки цілісності використовується геш-функція SHA-256.

Результати аналізу за критерієм “Безпека зберігання даних” наведено в таблиці 6.

Таблиця 6

«Безпека зберігання даних» для сервісу Wuala

Алгоритм шифрування даних	Конвергентна схема шифрування
Володіння ключем шифрування даних	Ключем зберігається на стороні клієнта

2.3 Аналіз сервісу зберігання даних Yandex.Disk

2.3.1 Вхід у систему та реєстрація

Для реєстрації і входу в систему використовується безпечний канал зв'язку.

Нові облікові записи можуть бути створені тільки на сторінці Яндекс. Для користування сервісом треба мати обліковий запис у системі Яндекс, що є єдиним для всіх додатків, у тому числі і Yandex.Disk.

Під час реєстрації користувач повинен обов'язково надати ім'я, інформацію про статтю, дату народження, придумати унікальний логін та двічі ввести пароль. Крім того необхідно обрати секретне питання та ввести інформацію з картинки. Використовується поштова скринька Яндекс, яка має бути унікальною для кожного облікового запису.

Існують обмеження на довжину пароля, яка має складатися як мінімум з шести символів і бути не більшим за 20 символів, пароль не може бути введено не на англійській розкладці клавіатури, та не повинен співпадати з логіном, інших обмежень немає.

Яндекс надає підказку про якість обраного пароля під час реєстрації, проте не відкидає слабкі паролі.

Оскільки логін є єдиним для всіх додатків Яндекс — додаткове підтвердження реєстрації не проводиться.

У разі невдалої спроби входу в систему Яндекс повідомляє користувача, що була введена не правильна пара логін/пароль.

Якщо користувач забув свій пароль, на альтернативну адресу електронної пошти надсилається URL сторінка для зміни паролю. Також можна використати секретний код, який висилається на альтернативну адресу пошти, якщо вона не зазначена — код надсилається на номер мобільного телефон, якщо він також не зазначений — використовується секретне питання. Функція входу надає можливості для збору інформації про вже зареєстровані імена.

Яндекс запобігає перебору паролів за допомогою вимоги обов'язкового вводу символів із зображення після серії невдалих спроб входу в систему.

В Yandex.Disk наразі не реалізовано механізму двофакторної автентифікації.

Результати аналізу сервісу Yandex.Disk за критерієм «Вхід у систему та реєстрація» наведено в таблиці 7.

Таблиця 7

«Вхід у систему та реєстрація» для сервісу Yandex.Disk

Мінімальна довжина пароля	6 символів
Захист від атаки перебору пароля	Використання символів із зображення після серії невдалих спроб входу в сервіс
Двофакторна автентифікація	Відсутня
Механізм відновлення пароля	Надсилається URL сторінки, на якій користувач може змінити пароль чи використовує секретний код

2.3.2 Захищений канал зв'язку

В ході аналізу сервісу Yandex.Disk був розглянутий принцип забезпечення захищеного каналу зв'язку між клієнтом та сервером, результати наведено у таблиці 8.

Таблиця 8

«Захищений канал зв'язку» для сервісу Yandex.Disk

Протокол формування захищеного каналу зв'язку	TLS 1.0
Алгоритм автентифікації повідомлень	RC4_128 (SHA1)
Алгоритм узгодження ключів	RSA (1024 біт)

2.3.3 Безпека зберігання даних

Yandex.Disk не використовує шифрування даних на стороні сервера. Результати аналізу за критерієм «Безпека зберігання даних» наведено в таблиці 9.

Таблиця 9

«Безпека зберігання даних» для сервісу Yandex.Disk

Алгоритм шифрування даних	Не використовується
---------------------------	---------------------

2.4 Аналіз сервісу зберігання даних SkyDrive

2.4.1 Вхід у систему та реєстрація

Для реєстрації і входу в систему використовується безпечний канал зв'язку.

Нові облікові записи можуть бути створені на сторінці SkyDrive. Для користування сервісом треба мати обліковий запис Microsoft. Обліковий запис є єдиним для додатків Hotmail, WindowsPhone, Xbox LIVE та SkyDrive.

Під час реєстрації, користувач повинен обов'язково надати ім'я та прізвище, інформацію про статі, дату народження, адресу електронної пошти та двічі ввести пароль. Крім того необхідно вказати, щонайменше, номер телефону чи секретне питання та ввести інформацію з картинки. Одна адреса електронної пошти може бути пов'язана з одним обліковим записом.

Для створення облікового запису Microsoft необхідно обрати пароль, який повинен включати не менше 8 і не більше 16 символів, які відносяться принаймні до двох з таких типів: букви верхнього і нижнього регістрів, цифри та символи. Крім того Microsoft відкидає поширені паролі. Під час створення пароля інформація про його якість не надається до моменту реєстрації.

Таким чином слабкі паролі не приймаються.

URL для підтвердження реєстрації передається на зазначену поштову скриньку, користування сервісом можливо лише після її підтвердження.

У разі невдалої спроби входу в систему Microsoft повідомляє який саме елемент було введено не правильно.

Якщо користувач забув свій пароль, йому надається 3 можливі способи для встановлення нового пароля: (1) на захищеній сторінці для встановлення нового пароля, URL якої відправляється на пошту; (2) за допомогою коду, який надсилається на мобільний телефон; (3) за допомогою заповнення анкети з великою кількістю секретних та особистих запитань.

Microsoft запобігає перебору паролів тимчасово блокуючи обліковий запис після багатьох невдалих спроб входу в заданий період часу.

Таблиця 10

«Вхід у систему та реєстрація» для сервісу SkyDrive

Мінімальна довжина пароля	8 символів
Захист від атаки перебору пароля	Тимчасове блокування
Двофакторна автентифікація	Пароль та одноразовий код доступу, що передається на альтернативну поштову адресу чи на мобільний телефон при вході з не довіреного пристрою
Механізм відновлення пароля	Надсилається URL сторінки, на якій користувач може змінити пароль чи використовує секретний код

Microsoft має можливість використання двофакторної автентифікації при вході з не довіреного пристрою, ця опція може бути включена в налаштуваннях профіля. Використовуються одноразові коди доступу, що їх можна отримувати на альтернативну поштову адресу чи на мобільний телефон.

Результати аналізу сервісу SkyDrive за критерієм «Вхід у систему та реєстрація» наведено в таблиці 10.

2.4.2 Захищений канал зв'язку

В ході аналізу сервісу SkyDrive був розглянутий принцип забезпечення захищеного каналу зв'язку між клієнтом та сервером, результати наведено у таблиці 11.

Таблиця 11

«Захищений канал зв'язку» для сервісу SkyDrive

Протокол формування захищеного каналу зв'язку	TLS 1.0
Алгоритм автентифікації повідомлень	AES_128_CBC (SHA1)
Алгоритм узгодження ключів	RSA (2048 біт)

2.4.3 Безпека зберігання даних

SkyDrive не використовує шифрування даних на стороні сервера. Результати аналізу за критерієм «Безпека зберігання даних» наведено в таблиці 12.

Таблиця 12

«Безпека зберігання даних» для сервісу SkyDrive

Алгоритм шифрування даних	Не використовується
---------------------------	---------------------

2.5 Аналіз сервісу зберігання даних GoogleDrive

2.5.1 Вхід у систему та реєстрація

Для реєстрації і входу в систему використовується безпечний канал зв'язку.

Нові облікові записи можуть бути створені на сторінці Google. Для користування сервісом треба мати обліковий запис Google, який є єдиним для всіх сервісів і прив'язаний до електронної адреси Gmail.

Під час реєстрації користувач повинен обов'язково надати ім'я та прізвище, інформацію про статі, дату народження, придумати унікальну

адресу електронної пошти та двічі ввести пароль. Крім того необхідно ввести інформацію з картинки. Одна адреса електронної пошти може бути пов'язана з одним обліковим записом.

Для створення облікового запису Google необхідно обрати пароль, який повинен включати не менше 8 і не більше 100 символів. У паролі можна використовувати латинські букви (як великі, так і малі: A-Z, a-z), цифри (0-9) і знаки пунктуації. Пароль може складатися із символів лише однієї групи. Під час створення пароля система надає підказку про якість пароля. Крім того Google відкидає поширені паролі.

Таким чином слабкі паролі не приймаються.

Оскільки логін є єдиним для всіх додатків Google— додаткове підтвердження реєстрації не проводиться.

У разі невдалої спроби входу в систему, Google повідомляє користувача, що один елемент з пари логін/пароль є не правильним, проте не уточнює який саме.

Якщо користувач забув свій пароль, йому надається 2 можливі способи для встановлення нового пароля: (1) на захищеній сторінці для встановлення нового пароля, URL якої відправляється на пошту; (2) за допомогою коду, який надсилається на мобільний телефон коротким повідомленням чи може бути повідомлений протягом телефонного дзвінка.

Google запобігає перебору паролів за допомогою вимоги обов'язкового вводу символів із зображення після серії невдалих спроб входу у сервіс.

Google має можливість використання двофакторної автентифікації, ця опція може бути включена в налаштуваннях профілю. Використовуються одноразові коди доступу, що їх можна отримувати на мобільний телефон.

Результати аналізу сервісу GoogleDrive за критерієм «Вхід у систему та реєстрація» наведено в таблиці 13.

Таблиця 13

«Вхід у систему та реєстрація»
для сервісу GoogleDrive

Мінімальна довжина пароля	8 символів
Захист від атаки перебору пароля	Використання символів із зображення після серії невдалих спроб входу в сервіс
Двофакторна автентифікація	Пароль та одноразовий код доступу, що передається на мобільний телефон
Механізм відновлення пароля	Надсилається URL сторінки на якій користувач може змінити пароль чи використовує секретний код

2.5.2 Захищений канал зв'язку

В ході аналізу сервісу GoogleDrive був розглянутий принцип забезпечення захищеного каналу зв'язку між клієнтом та сервером, результати наведено у таблиці 14.

Таблиця 14

«Захищений канал зв'язку» для сервісу GoogleDrive

Протокол формування захищеного каналу зв'язку	TLS 1.1
Алгоритм автентифікації повідомлень	RC4_128 (SHA1)
Алгоритм узгодження ключів	ECDHE_ECDSA (256 bit)

2.5.3 Безпека зберігання даних

GoogleDrive не використовує шифрування даних на стороні сервера. Результати аналізу за критерієм «Безпека зберігання даних» наведено в таблиці 15.

Таблиця 15

«Безпека зберігання даних» для сервісу GoogleDrive

Алгоритм шифрування даних	Не використовується
---------------------------	---------------------

2.6 Порівняльний аналіз сервісів зберігання даних у хмарі

Проаналізувавши сервіси за визначеними критеріями безпеки можна навести наступну підсумкову таблицю 16.

Таблиця 16

Підсумкова оцінка аспектів безпеки

	Вхід в систему та реєстрація	Захищений канал зв'язку	Безпека зберігання даних
Dropbox	±	++	±
Wuala	--	±	++
Яндекс Диск	-	+	--
SkyDrive	++	+	--
GoogleDrive	++	+	--

Кожен критерій безпеки оцінено з використанням таких візуальних позначок:

«++» означає, що всі вимоги виконано; «+» — всі базові вимоги виконано; «±» — більшість вимог виконано, проте є деякі проблеми; «-» — більшість вимог не виконано, «--» — жодна з умов не виконана.

ВИСНОВКИ

Метою роботи є аналіз існуючих широко поширених сервісів зі зберігання інформації в публічній хмарі з точки зору безпеки інформації. Для проведення були відібрані п'ять сервісів, а саме Dropbox, SkyDrive, GoogleDrive, Wuala та Яндекс.Disk. Загально визнано, що сервіси Dropbox, SkyDrive та Google Drive є найбільш популярні у світі. Сервіс Яндекс.Disk використовується переважно у країнах пострадянського простору. Сервіс Wuala вважається найбільш безпечним та надійним.

Аналіз сервісів зі зберігання інформації в публічній хмарі проводився за такими критеріями:

- вхід у систему та реєстрація;
- захищений канал зв'язку;
- безпека зберігання даних.

Аналіз показав, що з-поміж обраних рішень найвищий рівень безпеки інформації, дійсно, забезпечує сервіс Wuala, проте має певні обмеження на використання та відновлення пароля, найнижчий рівень захисту забезпечується рішенням від Yandex - Yandex.Disk, а сервіси Dropbox, SkyDrive та GoogleDrive можна назвати компромісними рішенням між безпекою інформації, функціональністю та зручністю застосування.

Література

- [1] J. W. Rittinghouse, J. F. Ransome, «Cloud Computing: Implementation, Management, and Security», 2009, CRC Press — 340 p.
- [2] T. Mather, S. Kumaraswamy, S. Latif, «Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance», O'Reilly Media, 2009.— 334 p.
- [3] M. Borgmann, T. Hahn, M. Herfert, T. Kunz, M. Richter, U. Viebeg, S. Vowe, «On the Security of Cloud Storage Services», Fraunhofer Institute SIT, 2012 — 143p.
- [4] D. Grolimund, L. Meisser, S. Schmid, R. Wattenhofer, «Cryptree: A folder trees structure for cryptographic file systems. In Reliable Distributed Systems», SRDS, 2006.
- [5] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, M. Theimer, «Reclaiming Space from Duplicate Files in a Server», Fraunhofer Institute SIT, 2012.

Надійшла до редколегії 26.04.2013



Погребняк Костянтин Анатолійович, кандидат технічних наук, доцент кафедри БІТ ХНУРЕ, начальник відділу КЗІ АТ «ІІТ». Наукові інтереси: застосування методів алгебраїчної геометрії в криптології, асиметричний криптоаналіз.



Повтарев Дмитро Валерійович, аспірант кафедри БІТ ХНУРЕ. Наукові інтереси: дослідження механізмів безпеки хмарних обчислень.

УДК 681.3.06

Анализ безопасности сервисов хранения данных в облаке / К.А. Погребняк, Д.В. Повтарев // Прикладная радиоэлектроника: науч.-техн. журнал. — 2013. — Том 12. — № 2. — С. 202—208.

Статья посвящена анализу сервисов хранения информации в облаке. Для анализа сервисов определяются критерии безопасности, по которым проводится сравнение. Рассматриваются следующие сервисы: Dropbox, SkyDrive, GoogleDrive, Wuala и Yandex.Disk. Основное внимание уделяется анализу интерактивного входа в систему, регистрации, формированию защищенного канала связи и механизмам безопасности хранения данных.

Ключевые слова: облачные вычисления, сервис хранения информации, безопасность хранения данных.

Табл.: 16. Библиогр.: 5 назв.

UDC 681.3.06

Analysis of security of cloud data storage services / K.A. Pogrebnyak, D.V. Povtariev // Applied Radio Electronics: Sci. Journ. — 2013. — Vol. 12. — № 2. — P. 202—208.

This paper is devoted to analyzing data storage services in the cloud. The security criteria are defined to analyze the services. The paper covers the following services: Dropbox, SkyDrive, GoogleDrive, Wuala and Yandex.Disk. The focus of the analysis is on an interactive login, registration, formation of a secure communication channel and data security mechanisms.

Keywords: cloud computing, information storage service, data storage security.

Tab.: 16. Ref.: 5 items.