– діти у віці 13-18 років, у першу чергу дівчатка з неповних та реструктурованих сімей (коли один із батьків нерідний).

Одержано 02.11.2018

УДК 681.3.06

Андрій Володимирович БІЛОБРОВ,
курсант 2 курсу групи Ф4-202 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ

БЕЗПЕКА ЗБЕРІГАННЯ ІНФОРМАЦІЇ В ХМАРНИХ СХОВИЩАХ

Хто володіє інформацією – той володіє світом – цей принцип, актуальний для всієї історії людства, наприкінці XX століття став актуальним як ніколи до цього. Нині відбулася трансформація суспільства із промислового на інформаційне суспільство. В умовах сучасного складного комплексно виробництва, високих темпів науково-технічного розвитку та інтенсивних потоків інформації керувати нею по-старому просто неможливо. Ось чому управління стало наукою, а переробка інформації – галуззю індустрії, що базується на сучасній обчислювальній техніці і є однією із найважливіших складових ефективного управління.

На даний час жоден серйозний проект не може обходитися без виконання регулярного резервного копіювання. Крім вибору і налаштування системи архівування даних потрібно визначитися де ці дані зберігати. Причому, бажано не на тому ж сервері де робить бекап (резервна копія), а мати можливість зберігати дані в якому-небудь незалежному надійному місці. Для цього ідеально підходять так звані хмарні сховища.

Хмарне сховище являє собою модель схову даних, де цифрові дані зберігаються в логічні пули, а фізичне зберігання охоплює кілька серверів (і часто на різних місцях (локаціях)), фізичне середовище, як правило, належить хостинговим компаніям, вони ж керують цим середовищем. Ці постачальники хмарних систем схову даних відповідають за схов наявної інформації й доступ до неї, та за роботу фізичного середовища. Користувачі купують у постачальників послуг хмарного сховища змогу зберігати там дані.

Як свідчать дослідження аналітичного агентства Gartner, основним напрямком і двигуном розвитку IT-індустрії хмарні технології стали з кінця 2009 року. 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. Хмарну безпеку сьогодні вважають одним з найперспективніших сервісів в інтернеті. Такі системи надають більшість можливостей звичним системам IT-безпеки, виносячи за дужки питання їх фізичного розміщення. Провайдери хмар обіцяють захист критично важливої інформації від крадіжки, витоку і втрати.

Питання безпеки даних давно стосуються не тільки рядових користувачів і великих організацій. Прорахунки можливі і на набагато більш серйозному рівні. В середині листопада проект по роботі з ризиками в кіберпросторі UpGuard повідомив, що 1,8 мільярда документів Пентагону виявилися незахищеними – через банальну помилку в налаштуваннях доступу. Інформація, яка, втім, не містила секретних даних, зберігалася на трьох публічних хмарних серверах. Цей випадок – ще один приклад того, що навіть організації такого рівня, які працюють з найважливішими відомостями, не застраховані від проблем, пов'язаних з безпекою даних. Малий і середній бізнес, відповідно, також не може не думати про ці проблеми.

«Якщо немає контролю над інфраструктурою, то немає і повної впевненості в тому, що постачальник рішення реалізує всі необхідні – або хоча б заявлені – організаційні та технічні заходи забезпечення кібербезпеки», – коментує архітектор систем інформаційної безпеки компанії IT-Інтегратор Олексій Швачка [2]. Відомі випадки, коли навіть найбільші хмари можуть «відмовити». У того ж Amazon було дві масштабних відмови в обслуговуванні – інфраструктура провайдера була недоступна протягом декількох годин.

Очевидно, ризики в хмарах існують. Але не варто думати, що тільки провайдер відповідає за безпеку. Найбільші гравці ринку, такі як Amazon, Microsoft і Google, гарантують в першу чергу фізичну безпеку дата-центрів і збереження даних клієнтів від руйнування. Клієнти ж відповідають за те, що відбувається на їх віртуальній ділянці хмари. Само собою, і провайдери, і незалежні постачальники систем безпеки надають цілий арсенал для цифрового захисту, але їх використання – прерогатива IT-відділів компаній і вимагає додаткового кваліфікованого персоналу і відповідних бюджетів.

У США підкреслюють, що перший крок до організації безпеки хмари – дослідження можливих загроз. Там також називають кілька ключових рішень для посилення хмарної безпеки. Серед них – шифрування даних, а також їх захист при передачі. Зашифрована інформація під час передачі повинна бути доступна тільки після автентифікації користувача з достатніми правами.

Крім традиційного пароля рекомендується використовувати додаткові кошти автентифікації, такі як токени і сертифікати. Також фахівці радять організувати максимально прозору і безпечну взаємодію провайдера з системами авторизації підприємства – такими як LDAP (Lightweight Directory Access Protocol) і SAML (Security

Assertion Markup Language). Варто пам'ятати і про важливість ізоляції користувачів в хмарному середовищі – найчастіше через можливі помилки в налаштуваннях або в коді програмного забезпечення, один користувач може отримати доступ до не своїх даних.

«Варто розуміти, що в сфері хмарних обчислень Україна знаходиться ще на самому старті і на роки відстала від світових тенденцій. Проте, останнім часом цей напрям розвитку IT-індустрії набирає обертів, тому зміни неминучі і до них життєво важливо починати підготовку вже зараз», – говорить Олександр Кардаков, віце-президент Асоціації Digital Ukraine.

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, AmazonCloudDrive, JungleDisk, GooglePlayMusic, MediaFire, Office365, Zoho, RapidShare, Sendspace, YouSendIt, Carbonite, Flickr, Photobucket, SmugMug, GoogleMusic, AppleiCloud, AmazonCloudPlayer.

Аналіз сервісів зі зберігання інформації в публічній хмарі 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 [1].

Таблиця 1

Оцінка аспектів безпеки найпоширеніших сервісів

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

В табл. позначено: «++» – всі вимоги виконано; «+» – більшість вимог виконано, проте є деякі проблеми; «-» – більшість вимог не виконано; «--» – жодна з умов не виконана.

Аналіз сервісів зі зберігання інформації в публічній хмарі проводився за такими критеріями: вхід у систему та реєстрація; захищений канал зв'язку; безпека зберігання даних.

Як стало зрозуміло, хмарне сховище має як багато переваг, так і велику кількість недоліків, однак це вагомий крок у сфері зберігання інформації і в подальшому розвитку його чекають кардинальні зміни.

Список бібліографічних посилань

1. Погребняк К А., Повтарєв Д. В. Аналіз безпеки сервісів зберігання даних у хмарі. Прикладная радиоэлектроника. 2013. Том 12, № 2. С. 202–208.

2. Хмарна безпека: чи згущуються хмари над захистом даних? // ООО «Видавничий дім "МЕДІА-ДК"». 12 грудня 2017 16:14. URL: https://biz.nv.ua/ukr/kibervoiny_i_biznes/hmarna-bezpeku-zgushchujutsja-chi-hmari-nad-zahistom-danih-2331588.html (дата звернення: 30.10.2018).

Одержано 30.10.2018

УДК 004.056.53

Михайло Юрійович БУРДІН,
доктор юридичних наук, професор,
проректор Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-6748-3321;
Юрій Валерійович ГНУСОВ,
кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-9017-9635;
Сергій Володимирович КАЛЯКІН,
завідувач навчальної лабораторії
кафедри кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0003-3946-0189

ОКРЕМІ АСПЕКТИ ПРОТИДІЇ КІБЕРАТАКАМ НОВОГО ПОКОЛІННЯ

Останнім часом фахівцями з кібербезпеки було відзначено значне зростання рівня небезпечності атак у кіберпросторі, що дало привід зробити висновки про появу кібератак нового покоління.

У лютому 2018 р. аналітики антивірусної компанії McAfee підрахували, що в 2017 р. світовий збиток від кіберзлочинів склав близько $ 600 млрд., або 0,8 % від світового ВВП, збільшившись приблизно на 35 % у порівнянні з оцінкою за 2014 рік, яка становила $ 445 млрд. Серед факторів, що зумовили зростання, фахівці перерахували таке: дедалі витонченіші хакерські атаки, розширення ринку кіберкримінальних послуг і поширення криптовалют. Експерти визнали, що найбільш швидко зростає такий вид кіберзлочинів, як атаки за допомогою вірусів-шифрувальників. Хакери все частіше вдаються до цього методу на тлі зростаючої доступності сервісів, побудованих за моделлю Ransomware-as-a-Service (RaaS, «Вимагання як послуга»). У McAfee нарахували понад 6 тис. кримінальних онлайн-ресурсів, які пропонують віруси-вимагачі та послуги з організації атак за їх допомогою.