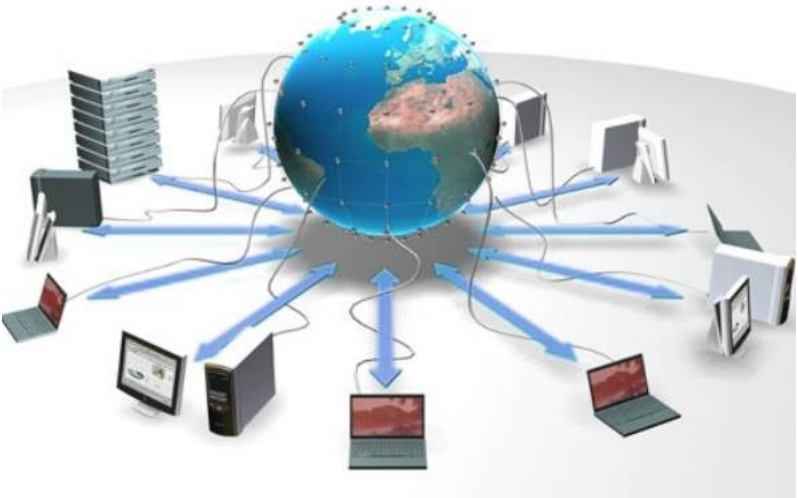
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

КАФЕДРА ЕКОНОМІЧНОЇ КІБЕРНЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ І УПРАВЛІННІ»

ЗБІРНИК НАУКОВИХ СТУДЕНТСЬКИХ ПРАЦЬ

ВИПУСК 3



Одеса
2021

СХОВИЩА ДАНИХ, ЇХ ОСОБЛИВОСТІ ТА РІВЕНЬ ЗАХИЩЕНОСТІ НА ПІДПРИЄМСТВАХ

Марініч А. В.[1], **Орлик О. В.**[2]

1 – студентка 3 курсу 35 гр., факультет міжнародної економіки,
2 – канд. екон. наук, доцент, кафедра економічної кібернетики та інформаційних технологій
Одеський національний економічний університет, м. Одеса

АНОТАЦІЇ

Марініч А. В., Орлик О. В. ***Сховища даних, їх особливості та рівень захищеності на підприємствах.*** *В статті розглянуто існуючі способи організації сховищ даних на підприємствах, в т. ч. хмарних. Наведено переваги та недоліки різних способів збереження даних на підприємствах. Проаналізовано сучасні тенденції розвитку ринку публічних хмарних сервісів та розглянуто особливості кожного з них.*
Ключові слова: *інформація, інформаційна система, сховище даних, хмарне сховище, криптографічні методи, шифрування.*

Маринич А. В., Орлик О. В. ***Хранилища данных, их особенности и уровень защищенности на предприятиях.*** *В статье рассмотрены существующие способы организации хранилищ данных на предприятиях, в т. ч. облачных. Наведены преимущества и недостатки различных способов хранения данных на предприятиях. Проанализированы современные тенденции развития рынка публичных облачных сервисов и рассмотрены особенности каждого из них.*
Ключевые слова: *информация, информационная система, хранилище данных, облачное хранилище, криптографические методы, шифрование.*

Marinich A., Orlyk O. ***Data warehouses, their features and the level of security at enterprises.*** *The article discusses the existing methods of organizing data warehouses in enterprises, including cloud ones. The advantages and disadvantages of various ways of storing data in enterprises are suggested. The current trends in the development of the public cloud services market are analyzed and the features of each of them are considered.*
Keywords: *information, information system, data storage, cloud storage, cryptographic methods, encryption.*

Марініч А. В., Орлик О. В. *Сховища даних, їх особливості та рівень захищеності на підприємствах //* Інформаційні технології в економіці і управлінні : зб. наук. студ. праць. Одеса : ОНЕУ, 2021. Вип. 3. С. 111–121.

Постановка проблеми у загальному вигляді. Розвиток корпоративних сховищ не задовольняє всім поставленим підприємствами вимогам. Ці вимоги формуються в результаті зміни законодавства в області зберігання інформації і пов'язані, в основному, із забезпеченням інформаційної безпеки. Крім цього, користувачі, що працюють з корпоративними інформаційними системами, хочуть від таких систем більш простого та зручного використання.

Аналіз досліджень і публікацій останніх років. Проблемами безпечного збереження даних в базах інформаційних систем займаються багато вітчизняних та зарубіжних науковців, серед яких: В. Глушков, М. Полтавцева, А. Хабаров, Л. Файнзільберг, В. Єсін, О. Кузнєцов, Л. Сорока та ін. Питання безпеки даних в хмарних сховищах знайшли відображення в працях: Є. Щербініної, Б. Марценюка, А. Філоненко, К. Вамсея, Р. Шрірама, П. Мелла, Т. Гранса, Дж. Ліклайдера, Дж. Маккарті та ін.

Як показав аналіз публікацій, проблема збереження корпоративної інформації в сховищах даних є на сьогодні досить актуальною і потребує подальших досліджень.

Виділення невирішених раніше частин загальної проблеми. Зважаючи на постійний прогрес в області зберігання інформації виникає необхідність дослідити поточний рівень розвитку корпоративних сховищ та визначити, наскільки вони задовольняють вимогам, що перед ними ставляться.

Мета статті. Мета статті полягає у дослідженні існуючих способів організації сховищ даних на підприємствах, виявленні їх переваг та недоліків, а також розгляді особливостей корпоративних хмарних рішень.

Виклад основного матеріалу дослідження. З розвитком цифрової техніки кількість інформації значно збільшується. Зараз практично кожна подія в нашому житті знаходить відображення в цифровому варіанті. В результаті цього людина не може вже обробляти, зберігати і передавати такі обсяги інформації без допомоги автоматизованих інформаційних систем, які представляють собою комплекс інформаційних, програмних, технічних, організаційно-методичних та інших необхідних засобів, що забезпечують збір, обробку, зберігання, передачу даних, а також маніпулювання ними для вирішення різних завдань. Далі під інформаційною системою ми будемо розуміти автоматизовану інформаційну систему.

Функціонування інформаційної системи забезпечує якесь сховище даних, в якому міститься вся інформація, що обробляється і надається цією системою.

Сховище даних являє собою сукупність програмно-апаратних засобів, що забезпечує зберігання даних, а також їх коректне надання керуючій системі. У разі необхідності забезпечення безперервної роботи інформаційної системи або високої цінності збережених даних може використовуватися резервне копіювання.

Можна виділити кілька основних типів інформаційних систем в залежності від призначення: корпоративні; персональні.

Сховище даних для інформаційної системи кожного типу буде мати деякі особливості реалізації.

Під корпоративною інформаційною системою розглядається інформаційна система масштабу підприємства. Головним завданням такої системи є інформаційна підтримка виробничих, адміністративних та управлінських процесів. Для корпоративних інформаційних систем часто використовуються сховища, що забезпечують захист файлів шляхом поділу доступу користувачів. Для приватної інформаційної системи використовуються хмарні сховища, що забезпечують доступ до інформації з будь-якого носія з виходом в мережу Інтернет, при проходженні ідентифікації і аутентифікації.

В якості заходів щодо захисту конфіденційності інформації застосовують криптографічні методи. Для кращого захисту інформації часто застосовують певну сукупність цих способів. Це дозволяє запобігти розкраданню інформації в разі несанкціонованого доступу до сховища.

Обмеження доступу до інформації в інформаційній системі не може повністю гарантувати її безпеку. Загрози інформаційній безпеці проявляються у можливих діях над інформаційною системою, які можуть завдати шкоди її безпеці. Тому інформаційна безпека ґрунтується на здійсненні заходів щодо забезпечення конфіденційності, цілісності та доступності інформації.

Конфіденційність – властивість інформації, при якому доступ до інформації можуть отримати тільки її законні користувачі.

Цілісність – властивість інформації, що гарантує можливість зміни інформації, що захищається тільки з боку її законних користувачів.

Доступність – властивість інформації, при якому здійснюється безперешкодний доступ для її законних користувачів.

Технології безпечного зберігання інформації (storage security) активно розвиваються останнім часом і на це є кілька причин:

– пристрої для зберігання інформації постійно зменшуються в розмірах, при цьому відбувається збільшення їх ємності. Це означає, що ступінь концентрації інформації зростає і в разі втрати носія втрачається більша частина даних;

– на сьогоднішній день вже склалося уявлення про те, як слід захищатися від зовнішніх загроз. Звичайно, ці проблеми як і раніше існують, але існують відпрацьовані методи і дії, які допомагають вибудувати захист від загроз і знизити ризик втрати інформації [1].

Системи безпечного зберігання даних спрямовані в першу чергу на безпеку даних при фізичному доступі зловмисника до носіїв інформації. Ризик виникнення подібної ситуації може здатися досить невеликим, проте існує кілька цілком можливих варіантів:

– розміщення сервера в сторонньому дата-центрі (від англ. data center);

– ремонт і утилізація носіїв;

– втрата або крадіжка обладнання або носіїв.

У першому випадку необмежений фізичний доступ до сервера має компанія, що надає послугу зберігання, є третьою особою і не відноситься до організації, що зберігає свої дані.

У двох останніх випадках зловмисник отримує доступ до інформації безпосередньо з носія. При ремонті носія зловмисник може спробувати відновити інформацію на жорсткому диску. А в разі крадіжки зловмисник вже має доступ до інформації з носія без особливих труднощів. Тому деякі організації не передають жорсткі диски, що вийшли з ладу, в ремонтні центри, а відразу знищують їх і замінюють на нові.

Найбільш очевидним рішенням всіх зазначених проблем є шифрування. Зрозуміло, ключ шифрування повинен бути секретним і зберігатися окремо від зашифрованої інформації. Залежно від того, що конкретно потрібно шифрувати, вибирається технологія шифрування. Можна шифрувати розділи даних цілком, або окремо шифрувати файли і папки. Останній варіант є більш гнучким, так як крім шифрування є можливість використовувати поділ доступу до файлів. Однак, це викликає додаткові складності, пов'язані із створенням, розповсюдженням і зберіганням ключів користувачів.

При генерації ключів шифрування найкращим варіантом є використання фізичного генератора випадкових чисел, але на практиці цей спосіб є важкореалізованим.

Для зберігання ключів сучасні системи використовують смарт-карти і USB-пристрої з захищеною PIN-кодом пам'яттю. Для використання ключа, що зберігається на пристрої, користувач повинен ввести коректний PIN-код, а кілька невдалих спроб поспіль призводять до блокування пристрою.

Також слід зазначити особливість – кворум ключів, зустрічається в системах досить рідко. Вона дозволяє розбивати ключ шифрування на кілька складових частин, причому для відновлення оригінального ключа необхідні не всі частини. Дана технологія дозволяє знизити ризик розкриття ключа шифрування і забезпечити більший рівень доступності даних.

Найбільш простий і найпоширеніший варіант – це локальне зберігання інформації на персональному комп'ютері, використовуючи місце на жорсткому диску. Очевидним недоліком такого способу зберігання інформації є те, що працювати з даними можна тільки з цього персонального комп'ютера. При зберіганні інформації на зовнішньому носії доступ до інформації вже не залежить від можливості роботи на конкретному комп'ютері, але значно збільшується можливість втрати інформації в результаті технічної несправності носія або його втрати. Останнє також може привести до розголошення інформації, що досить часто є неприпустимим.

Для більш зручного способу зберігання інформації та забезпечення доступу до неї використовують локальні мережі. Наявність загального доступу до ресурсу забезпечує можливість його спільного використання з будь-якого персонального комп'ютера, що знаходиться в мережі. Таким мережевим ресурсом може бути папка, в якій зберігається інформація.

Однак комп'ютер, на якому знаходиться така папка, весь час повинен бути доступний, тобто включений і мати постійне підключення до локальної мережі.

Тому, якщо існує необхідність постійного доступу до даних декількох користувачів, використовують сервери для зберігання інформації. Сервери дозволяють зберігати досить великі обсяги інформації, на відміну від персональних комп'ютерів або переносних носіїв. Тому створення сховищ даних з використанням серверів досить часто застосовується на підприємствах.

На сьогоднішній день, кожна людина, яка активно використовує персональний комп'ютер, так чи інакше стикалася з хмарними технологіями. З'явившись близько 10 років тому, перші хмарні сховища істотно змінили уявлення користувачів щодо зберігання інформації.

Хмарний сервіс для користувача являє собою якийсь простір на віддаленому сервері, в якому він може працювати зі своїми файлами, завантажуючи і видаляючи їх, а також надаючи іншим користувачам в спільний доступ.

Незважаючи на те, що хмарні сховища з'явилися відносно недавно, вони широко поширені серед користувачів, що працюють з інформацією, до якої часто потрібен доступ. Відмінність від попередніх способів зберігання інформації в тому, що користувач може працювати з інформацією з будь-якого пристрою (персональний комп'ютер, планшет і т. д.), що має доступ в Інтернет.

Для користувача використання «хмари» досить зручно, тому що йому виділяється певний обсяг пам'яті, представлений однією папкою. Користувач працює в «хмарі», при цьому він не знає, де саме зберігатися його інформація. Для користувача «хмара» – це його папка. З вищезазначеного випливає, що створення хмарних сховищ – це найбільш перспективна технологія зберігання інформації.

Система зберігання даних в «хмарі» використовує розподілене зберігання даних на серверах. Звідси виникають загрози безпеці інформації, що зберігається, але, зазвичай, інформація користувачів не має особливої цінності, на відміну від корпоративної інформації.

Зручність хмарних сервісів призводить до використання публічних хмарних сховищ працівниками в своїй роботі. Вони не замислюються про збереження інформації, забезпечення її безпеки. Такий стан справ, в кращому випадку викликає суперечки між різними службами компанії, а в гіршому – призводить до порушення системи безпеки. Крім загрози безпеці, використання працівниками публічних хмарних сервісів призводить до проблем, пов'язаних із законодавством. Простими заборонами виправити таку ситуацію досить складно. Компромісом може стати використання корпоративних хмарних сервісів як елемента інформаційної інфраструктури компанії [2].

Завдання зберігання інформації на підприємстві, звичайно, не обмежується тільки можливістю колективного доступу до файлів. Крім цього, сховище інформації має бути достатнього обсягу, щоб справлятися з постійно зростаючою кількістю інформації.

У відповідь на зростаючу потребу з боку компаній, на ринку поступово з'являються різні пропозиції в області хмарних технологій для підприємств.

Головною перевагою хмарного зберігання даних для компанії, є готова інфраструктура хмари. Це дозволяє компанії економити на затратах, пов'язаних з розробкою власних сервісів.

Світовий ринок хмарних рішень і послуг зростає настільки інтенсивно, що передбачити темп його збільшення виявляється на практиці досить важко, тому дані провідних аналітичних компаній часом сильно різняться. Проте, всі вони фіксують одні й ті ж тенденції: швидкий темп зростання витрат на cloud computing (хмарні обчислення), а також супутнього ринку сервісів, центрів обробки даних і трафіку даних в таких системах.

У квітні 2017 року аналітична компанія 451 Research опублікувала результати дослідження, які показали нову цінову війну, яку розв'язали лідери ринку хмарних обчислень. У повідомленні від 20 квітня 2017 року говориться, що, якщо раніше цінова конкуренція розвивалася тільки в сегменті віртуальних машин в хмарі, то тепер вона торкнулася сервісів зберігання даних [3].

Хмарні сервіси, представлені на ринку, можна розділити на кілька основних видів залежно від послуг, що надаються.

PaaS (платформа як послуга) – модель надання хмарних обчислень, при якій споживач отримує доступ до використання інформаційно-технологічних платформ: операційних систем, систем управління базами даних, програмного забезпечення, засобів розробки і тестування, розміщеним у хмарного провайдера. У цій моделі вся інформаційно-технологічна інфраструктура, включаючи обчислювальні мережі, сервери, системи зберігання, цілком керується провайдером. Провайдером так само визначається набір доступних для споживачів видів платформ і їх керованих параметрів. Споживачеві можуть використовувати платформи на свій розсуд, створюючи їх віртуальні екземпляри, встановлюючи, розробляючи і тестуючи на них прикладне програмне забезпечення. При цьому існує можливість динамічної зміни кількості споживаних обчислювальних ресурсів.

PaaS надає середу, яку розробники використовують для розробки або налаштування хмарних додатків. PaaS дозволяє розробникам створювати додатки з використанням вбудованих компонентів програмного забезпечення.

Найчастіше, PaaS використовується програмістами, які спільно працюють над різними проектами. В цьому випадку всі або частина розробників отримують доступ до єдиного середовища розробки віддалено. Відповідно, всі вони потребують в достатній кількості системних ресурсів, а також інструментів спільної роботи.

Надаючи інфраструктуру як послугу, PaaS пропонує ті ж переваги, що і IaaS. Однак додаткові компоненти створюють такі додаткові переваги, як:

– скорочення часу програмування;
– можливості розробки без збільшення числа співробітників;
– спрощена розробка для декількох платформ, включаючи мобільні платформи;
– економічне використання просунутих засобів;
– підтримка географічно розподілених команд розробників;
– ефективне управління життєвим циклом додатків [4].

DBaaS (Databaseas a Service, база даних як послуга) – це різновид PaaS. Використовуючи DBaaS, користувач може отримати доступ до бази даних будь-якого типу за запитом. Користувач може швидко розгорнути базу даних на будь-якому класі устаткування в середовищі, обраної ним програмної платформи (операційної системи). Компанія IBM, наприклад, надає доступ до масштабованої і повністю керованої бази даних через об'єктно-орієнтовані API.

SaaS (програмне забезпечення як послуга) – одна з форм хмарних обчислень, модель обслуговування, при якій передплатникам надається готове прикладне програмне забезпечення, яке повністю обслуговується провайдером. Постачальник в цій моделі самостійно управляє додатком, надаючи замовникам доступ до функцій з клієнтських пристроїв, як правило через мобільний додаток або веб-браузер.

Основні переваги моделі SaaS для споживача послуги:

– відсутність витрат, пов'язаних з установкою (користувачу не потрібно інсталювати програму на свій комп'ютер), оновленням (розробник буде завжди своєчасно оновлювати потрібні файли) і підтримкою працездатності обладнання і працюючого на ньому програмного забезпечення;
– надійність, яка обумовлена, тим, що основна частина апаратних функцій на серверах постачальника дублюється. Тобто, якщо на стороні постачальника вийшов з ладу жорсткий диск, можна бути впевненим, що важлива інформація вже записана на резервні носії, що належать контрагенту;
– універсальність: можливість одночасного користування одним і тим же інтерфейсом декількома користувачами; користувач може працювати з потрібними інтерфейсами з будь-якого комп'ютера. Багато з постачальників SaaS адаптують інтерфейси відповідного програмного забезпечення не тільки до користування на звичайному комп'ютері, але також і до специфіки мобільних пристроїв – смартфонів, планшетів;
– економічна вигода: у багатьох випадках SaaS-програми дешевше, ніж «коробкові» версії програмного забезпечення [5].

Прикладом SaaS може служити MicrosoftOffice 365. Корпорація Microsoft надає за моделлю SaaS доступ клієнтам до MS OfficeSuite (OfficeWebApps) поряд з SharePointServer, ExchangeServer і іншими сервісами та додатками.

IaaS (інфраструктура як послуга) надається як можливість використання хмарної інфраструктури для самостійного управління ресурсами обробки, зберігання, мережами та іншими фундаментальними обчислювальними ресурсами. Наприклад, споживач може встановлювати і запускати довільне програмне забезпечення, яке може включати в себе операційні системи, платформне і прикладне програмне забезпечення. Споживач може контролювати операційні системи, віртуальні системи зберігання даних і встановлені програми, а також володіти обмеженим контролем над набором доступних мережевих сервісів (наприклад, фаєрволом, DNS). Контроль і управління основною фізичною і віртуальною інфраструктурою хмари здійснюється хмарним провайдером [6].

У цьому випадку постачальник послуги надає в оренду обчислювальні ресурси. Це може бути сукупність віртуальних машин, сховищ даних, мережевих елементів різних типів. За допомогою IaaS користувач отримує можливість швидко розгортати копії ОС, запускаючи віртуальні копії ряду програмних пакетів. У цьому випадку немає необхідності розгортати власну мережеву інфраструктуру. Все необхідне можна отримати у постачальника IaaS. При цьому таке середовище практично завжди є гнучким і масштабованим.

Нещодавно з'явився новий сервіс щодо захисту хмарних сховищ для бізнесу – Securityas a Service (SecaaS). Securityas a Service – це бізнес-модель, в якій сервіс-провайдер послуг безпеки інтегрує свої сервіси в корпоративну інфраструктуру замовника. Напрями цієї послуги – це антивірусна і антиспам-фільтрація електронної пошти в хмарі, сервіси по захисту від DDoS-атак. Все більше підсистем безпеки йдуть в хмару, так як це дозволяє захищати дані в нових IT-системах і пристосовуватися до мінливої IT-інфраструктури [7].

У серпні 2020 року аналітична компанія IDC випустила дослідження, присвячене глобальному ринку публічних хмарних сервісів. За даними цих досліджень, представлених нами на рис. 1, у 2019 р. обсяг галузі склав 233,4 млрд дол. Це на 26% більше у порівнянні з результатом за 2018 рік, коли дохід дорівнював 185,2 млрд дол. Більшу частку ринку утримують сервіси SaaS. На них у 2019 році припадало приблизно 148,5 млрд дол., або 63,6% від загального розміру зафіксованої виручки. На другому місці знаходяться платформи IaaS з 49,0 млрд дол. і 21,0% галузі. Ще 35,9 млрд дол. принесли рішення PaaS, на частку яких припало 15,4% [3].

Слід зазначити, що світовий ринок хмарних рішень і послуг зростає настільки інтенсивно, що передбачити темп його збільшення виявляється на практиці досить важко, проте, спостерігаються одні й ті ж тенденції: швидкий темп зростання витрат на cloud computing, а також супутнього ринку сервісів, ЦОДів і трафіку даних в таких системах.

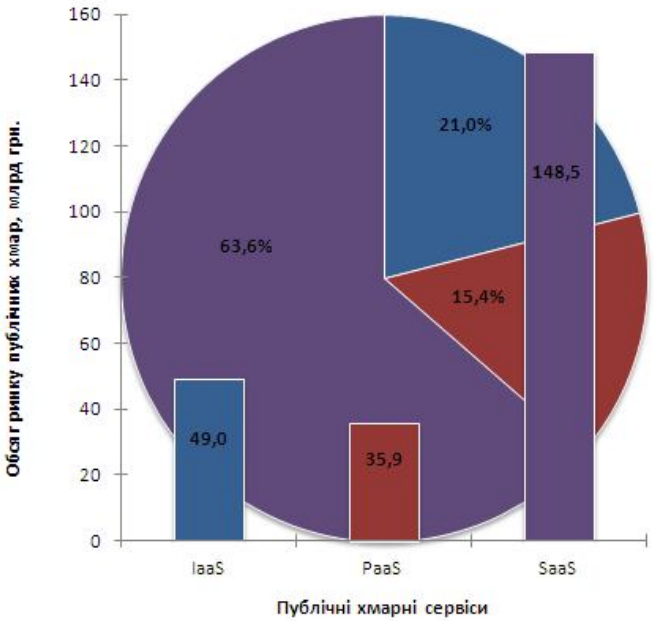


Рис. 1. Ринок публічних хмарних сервісів у 2019 р.

Джерело: розроблено авторами за даними [3]

Незважаючи на активний розвиток хмарних технологій в світі, для нашої країни «хмари» як корпоративний сервіс досі є чимось новим. Поширення широкосмугових мереж доступу в Інтернет вирішило основні проблеми використання хмарних технологій. Зараз практично кожен користувач має високошвидкісне підключення до Інтернету, причому постійно і з будь-якого пристрою. І, якщо користувачі активно використовують публічні хмарні сховища в особистих цілях, то організації не досить довіряють хмарним технологіям, щоб зберігати за їх допомогою корпоративні дані. Звичайно, ці побоювання не безпідставні, враховуючи, що дані, які зберігаються в «хмарі», фактично належать компанії-провайдеру, яка володіє сервером.

Однак, з кожним роком все більше організацій розуміють зручність використання хмарних технологій.

Більшість розвинених IT-компаній намагаються запропонувати свої рішення в області хмарних технологій. Однак, незважаючи на помітну зручність у використанні, «хмари» погано захищені з точки зору інформаційної безпеки. Для доступу до даних в хмарі користувачеві потрібно ввести тільки логін і пароль, які можуть бути вкрадені зловмисником за допомогою різних технічних засобів або зламані шляхом перебору. І навіть якщо користувач акуратно використовує свій логін і пароль, пароль

має хорошу захищеність від злому шляхом перебору, це зовсім не гарантує збереження даних, що зберігаються в хмарі. Розглянутий випадок лише ускладнює зловмисникові доступ в хмару через обліковий запис користувача, але не виключає можливості доступу до даних.

Дослідження комп'ютерної безпеки за останні 10 років показали, що зловмисникам не потрібно бачити дані користувача, щоб вкрасти їх [8]. Ризик таких атак особливо актуальний в хмарі, де у користувача немає контролю над додатками, з якими його файли ділять простір на сервері. Зловмисник може просто завантажити невеликі програми на кілька хмарних серверів. Ці програми не роблять нічого, крім шпигунства за даними інших користувачів. Для усунення цієї проблеми пропонуються різні рішення. Найбільш очевидний спосіб для підприємства – це використання власних серверів для зберігання інформації, які знаходяться у внутрішній мережі і відповідно не доступні для такого роду атак.

Ще однією особливістю використання хмарних сервісів є те, що користувачі, як правило, не мають поняття, де зберігаються їх файли і наскільки забезпечена безпека їх зберігання. Тому фахівці в області інформаційних технологій все частіше пропонують використовувати шифрування файлів, що зберігаються на серверах, причому для шифрування різної інформації одного і того ж користувача застосовувати різні ключі. А так як на сьогоднішній день для доступу в хмару часто застосовується веб-інтерфейс, то виникають складності в реалізації запропонованого підходу. Однак, найбільш простий підхід до шифрування, без передачі секретних ключів для доступу в хмару, вже реалізований і використовується деякими компаніями.

Корпоративне рішення в області хмарних сховищ даних має ряд переваг перед зберіганням даних на сервері в локальній мережі підприємства, яке зараз використовується в більшості випадків. В результаті роботи можна спроектувати доцільне у використанні організації хмарне сховище, яке дозволить спростити роботу користувачів, безпосередньо працюючих зі сховищем, а також підвищити рівень інформаційної безпеки.

Висновки з даного дослідження. Забезпечення безпеки інформації в інформаційних системах вимагає створення захищених сховищ даних, які являють собою сукупність програмно-апаратних засобів, що забезпечують зберігання даних, а також їх коректне надання. Способи організації цих сховищ розрізняються залежно від самої інформаційної системи.

Сховище даних повинно забезпечувати: зберігання різнорідної інформації на власних ресурсах, з можливістю поділу користувачів за рівнем доступу до даних, а також можливість роботи користувача зі своїми даними з будь-якого комп'ютера всередині мережі підприємства.

Для підвищення безпеки інформації використовують криптографічні методи, застосування яких спрямовано на усунення недоліків забезпечення безпеки під час використання сховищ даних.

ЛІТЕРАТУРА

1. Обзор технологий защиты информации при хранении. URL: https://www.osp.ru/winitpro/2007/07/4558994/ (дата звернення: 24.11.2020).

2. Колосков С., Абашев А., Мельник Р. Риски и тенденции в сфере обеспечения информационной безопасности // Информационная безопасность. 2013. № 1. С. 8.

3. Облачные вычисления (мировой рынок) // Tadviser, 20/08/2020. URL: https://www.tadviser.ru/index.php/Статья:Облачные_вычисления_(мировой_рынок) (дата звернення: 24.11.2020).

4. Что такое PaaS? URL: https://azure.microsoft.com/ru-ru/overview/what-is-paas/ (дата звернення: 24.11.2020).

5. SaaS – что это такое? Software as a Service – программное обеспечение как услуга. URL: http://fb.ru/article/187934/saas---chto-eto-takoe-software-as-a-service-programmnoe-obespechenie-kak-usluga (дата звернення: 24.11.2020).

6. Cloud Computing: What is Infrastructure as a Service. URL: https://technet.microsoft.com/en-us/library/hh509051.aspx (дата звернення: 21.11.2020).

7. Безкоровайный Д. Знакомимся с SecaaS – преимущества безопасности из облака. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/SecaaS_security_cloud_computing (дата звернення: 24.11.2020).

8. Hardesty L. Cloud security reaches silicon. URL: http://news.mit.edu/2015/cloud-security-chips-0223 (дата звернення: 24.11.2020).

9. Фінансово-економічна безпека підприємств та інформаційні технології забезпечення безпеки : монографія / О. В. Орлик, О. О. Кюне, О. Г. Єсіна, А. Ю. Вакула. Одеса : ФОП Гуляєва В.М., 2018. 140 с.

10. Орлик О. В. Проблеми забезпечення інформаційної складової економічної безпеки сучасних підприємств // Кібербезпека в Україні: правові та організаційні питання : матеріали III Всеукр. наук.-практ. конф. (Одеса, 30 листопада 2018 р.). Одеса : ОДУВС, 2018. С. 79–81.

11. Сохадзе Т. Т., Орлик О. В. Методи забезпечення безпеки інформації в інформаційних системах // Інформаційні технології в економіці і управлінні : зб. наук. студ. праць. Одеса : ОНЕУ, 2019. Вип. 1. С. 84–88.

12. Браїла Г. В., Орлик О. В. Ризики впровадження і використання інформаційних технологій на підприємствах // Інформаційні технології в економіці і управлінні : зб. наук. студ. праць. Одеса : ОНЕУ, 2020. Вип. 2. С. 58–67.

13. Antonopoulos N., Gillam L. Cloud Computing: Principles, Systems and Applications. L. : Springer, 2010. 379 p.

14. Vamsee K. Y., Sriram R. Data Security in Cloud Computing // Journal of Computer and Mathematical Sciences. 2011. Vol. 2 (1), pp. 15–23.

15. Storage Technologies Overview. URL: https://technet.microsoft.com/en-us/library/dn610883(v=ws.11).aspx (дата звернення: 21.11.2020).

16. Shcherbinina Ye., Martseniuk B., Filonenko A. Безпека бази даних і вивчення методів шифрування даних в хмарному сховищі // Системи управління, навігації та зв'язку : зб. наук. пр. Полтава : ПНТУ, 2020. Т. 3 (61). С. 104–106. DOI: https://doi.org/10.26906/SUNZ.2020.3.104.