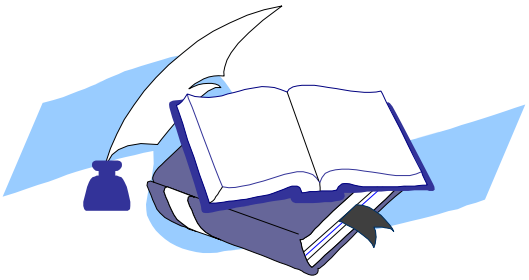
ІНФОРМАЦІЙНИЙ БЮЛЕТЕНЬ
№ 2 , 2019



Інститут інформаційних технологій і засобів навчання
НАПН України
Відділ компаративістики інформаційно-освітніх інновацій

БЕЗПЕКА ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ В ОСВІТІ

Впровадження та вдосконалення інформаційних технологій займає важливе місце серед численних інноваційних напрямків розвитку навчання і освіти в цілому. Розробляється безліч інформаційних сервісів, які вчитель може впроваджувати і ефективно використовувати в навчальному процесі та для свого професійного розвитку. Одним з перспективних напрямків розвитку сучасних інформаційних технологій є хмарні технології, які роблять доступним освітній контент для студентів, школярів і вчителів, служать для зберігання і синхронізації файлів, управлінням навчальним процесом, зберігання закладок і заміток; керування часом тощо. Проте "хмара" часто прихована за програмами, такими як "платформа для навчання" або "інформаційна платформа" (наприклад bettermarks [1] або SchulCommSy [2]) .

Такі IT-послуги пропонують та експлуатуються компаніями, що мають офіси у Німеччині, в ЄС або за межами Європи. У рідкісних випадках такі сервіси використовуються державними органами (наприклад, шкільними радами, школами чи іншими установами).

Багато шкіл користуються такими хмарними сервісами, але не займаються питаннями захисту даних, можливо, це пов'язано з тим, що технічні аспекти такого хмарного сервісу невідомі. Але захист інформації є дуже важливим, оскільки використовуються особисті дані учнів та вчителів, навчальні матеріали та результати навчання, всі ці дані автоматично обробляються за допомогою хмарного сервісу. Необхідно відмітити, що використання хмарних сервісів в освітньому процесі мають ряд переваг, серед яких:

- можливість доступу до даних з будь-якого комп'ютера, що має вихід в Інтернет;
- можливість організації спільної роботи з даними різних учасників навчального процесу;
- висока ймовірність збереження даних навіть у разі апаратних збоїв;
- освітні організації мають можливість безкоштовно використовувати хмарні сервіси;
- немає необхідності займатися придбанням, підтримкою та обслуговуванням

власної інфраструктури зі зберігання даних, що, в кінцевому рахунку, зменшує загальні витрати;

– процедури з резервування та збереження даних виробляються провайдером «хмарного» центру, яка не втягує в цей процес користувача цих послуг.

Важливим фактором є те, що в призначених для користувача угодах хмарних сервісів ніколи не містяться зобов'язання щодо збереження конфіденційності і цілісності даних. Користувачам цих послуг слід пам’ятати про необхідність забезпечувати весь комплекс вимог по обробці та захисту персональних даних, що не завжди реалізується в хмарі.

Основні ключові загрози хмарної безпеки за версією Cloud Security Alliance [5] (CSA - некомерційна організація, лідер в області стандартів, рекомендацій та ініціатив, спрямованих на підвищення безпеки і захищеності використання хмарних обчислень), з якими стикаються ті чи інші організації, що використовують хмарні сервіси, а саме:

1. витік даних - через велику кількість даних, які переносяться в хмари, майданчики хмарних хостинг-провайдерів стають привабливою метою для зловмисників (серйозність потенційних загроз безпосередньо залежить від важливості і значимості даних, що зберігаються), а втрата цих даних завдає значної шкоди репутації окремо взятої компанії;

2. компрометація (доступ сторонньої особи до інформації) облікових записів і обхід аутентифікації (процедура перевірки справжності) - витік даних найчастіше є результатом недбалого ставлення до механізмів організації перевірки автентичності, коли використовуються слабкі паролі, а управління ключами шифрування і сертифікатами відбувається неналежним чином (наприклад, коли кінцевим користувачам призначаються значно більші повноваження, ніж в дійсності необхідно або коли користувач переводиться на іншу позицію або звільняється, але при цьому не змінюється повноваження згідно з новими ролями);

3. зламування інтерфейсів та API - від того, наскільки добре відпрацьовані механізми контролю доступу, шифрування в API, залежить безпека і доступність хмарних сервісів (при взаємодії з третьою стороною, що використовує власні інтерфейси API, ризики значно зростають, оскільки виникає необхідність надавати додаткову інформацію, таку як, логін та пароль користувача);

4. вразливість використовуваних систем - проблема, яка трапляється в мультіарендних (елемент архітектури програмного забезпечення, де єдиний екземпляр додатку, запущеного на сервері, обслуговує безліч організацій-

клієнтів «орендарів») хмарних середовищах та вирішується за допомогою регулярного сканування на виявлення вразливостей, застосування останніх патчів і швидкої реакції на повідомлення щодо загрози безпеці;

5. викрадення облікових записів - сервісні акаунти і облікові записи користувачів необхідно контролювати, детально відстежуючи виконувані транзакції (група логічно об'єднаних послідовних операцій по роботі з даними, що обробляється або скасовується повністю);
6. інсайдери-зловмисники - інсайдерська загроза може виходити від нинішніх або колишніх співробітників, системних адміністраторів, підрядників або партнерів по бізнесу (у випадку з хмарою зловмисники можуть повністю або частково зруйнувати інфраструктуру, отримати доступ до даних);
7. цільові кібератаки – це напад хакерів на обраний об’єкт, що призводить до втрати та розкриття цінної інформації;
8. перманентна втрата даних - хмарні хостинг-провайдери для дотримання заходів безпеки рекомендують відокремлювати призначені для користувача дані від даних додатків, зберігаючи їх в різних локаціях, а також не варто забувати про ефективні методи резервного копіювання на зовнішні альтернативні захищені майданчики;
9. недостатня обізнаність - коли команда розробників з боку клієнта недостатньо знайома з особливостями хмарних технологій і принципами розгортання хмарних додатків, виникають операційні та архітектурні проблеми;
10. зловживання хмарними сервісами - хмари можуть використовуватися легітимними і нелегітимними організаціями, а метою останніх є використання хмарних ресурсів для здійснення зловмисних дій: запуску DDoS-атак, відправки спаму, поширення шкідливого контенту тощо;
11. DDoS-атаки - в результаті DoS-атак може сильно сповільнитися або зовсім припинитися робота значущих для споживача послуг сервісів;
12. спільні технології, загальні ризики - поставщики хмарних послуг надають віртуальну інфраструктуру, хмарні додатки, але якщо на одному з рівнів виникає вразливість, вона впливає на все оточення.

Дебра Литлджон Шиндер (Debra Littlejohn Shinder), яка є авторкою низки книг з комп'ютерних операційних систем, мереж та безпеки, у своїй статті "П'ять способів захистити себе в багатофункціональному, багатоплатформенному світі" [3] та Філіп Шауманн (Philipp Schaumann), спеціаліст з інформаційних технологій та

інформаційної безпеки, викладач в Дунайському університеті в Кремсі та Університеті прикладних наук Хагенберг, в статті «Як захистити себе при використанні хмарних сервісів?» [4] надають поради щодо захисту своїх даних та інформації у віртуальному просторі. Ось деякі з них:

1. ***Захист паролем*** – задайте унікальний та надійний пароль для кожного сервісу та включайте дворівневу автентифікацію (процедура перевірки автентичності) всюди, де це можливо (ім'я користувача плюс пароль або PIN-код як і раніше є найбільш поширеним способом, за допомогою якого ми автентифіціруємо себе системами, мережами, сайтами та службами). Зловмисник може отримати доступ до вашого пароля різними способами: шкідливі програми, ключі для реєстрації даних, груба сила, соціальна інженерія.

2. ***Налаштування пристрою*** – є безліч різних обчислювальних пристроїв, різних операційних систем та різних версій ОС, неможливо включити кожен з них. Ось деякі загальні поради щодо захисту мобільних пристроїв: виберіть модель свого мобільного пристрою з урахуванням безпеки та дізнайтеся, які пристрої підтримують віддалене стирання, шифрування файлів, двофакторну автентифікацію та інші функції безпеки; тримайте свої пристрої під контролем та не залишайте їх без уваги на "хвилину" на конференціях або ділових зустрічах, не позичайте їх іншим без вашого прямого нагляду; захистіть свої дані у разі крадіжки пристрою, на ноутбуках увімкніть програми BitLocker або інші програми шифрування, на планшетах і смартфонах, увімкніть захист пароля / PIN-коду; якщо ваш пристрій пропонує двофакторну автентифікацію, наприклад, відбиток пальців або розпізнавання обличчя, використовуйте її, встановіть програму відстеження та блокування мобільних пристроїв, увімкніть можливості віддаленого стирання, регулярно створюйте резервну копію даних на вашому комп'ютері. Вимкніть мережі та послуги, які вам не потрібні (wi-fi, bluetooth, інфрачервоний зв'язок, мобільні мережі, обмін файлами). Якщо у вас ввімкнено Bluetooth, встановіть його в нерозпізнаний режим. Встановіть доступ до електронної пошти до зашифрованого з'єднання. Переконайтеся, що на пристроях Android вимкнено налагодження USB. Переконайтеся, що резервне копіювання iPhone налаштовано на зашифроване. Встановіть PIN-код на SIM-карті, щоб його не можна було використовувати на іншому пристрої.

3. ***Бездротова служба безпеки.*** Ретельно оцініть дані, які ви помістили в хмарі. Не зберігайте там дуже цінні дані. Не зберігайте там *єдину* копію ваших даних, робіть резервне копіювання. Ретельно оцінюйте постачальників хмар, які ви вирішили використовувати. Попередньо ознайомтеся з опублікованими гарантіями та безпекою надання послуг: шифрування даних, яка інформація зберігається на серверах, ознайомтеся з їх умовами обслуговування та політикою

конфіденційності. Зрозумійте, що жодна хмарна служба (і, звичайно, не безкоштовне хмарне сервісне обслуговування) не надає вам повної гарантії щодо безпеки ваших даних. Порушення відбуваються.

4. Загальне анти-шкідливе ПЗ

Це категорія з порадами щодо захисту ваших пристроїв від багатьох типів атак, які поширені на сьогодні:

- завжди застосовуйте оновлення програмного забезпечення якомога швидше та запустіть антивірусне і антишпигунське програмне забезпечення;
- необхідно бути обережними при встановленні нових програм, попередньо ознайомтеся з відгуками, прочитайте інформацію про те де і як вони використовуються та не дозволяйте програмам автоматично оновлюватися, якщо ви не впевнені, що довіряєте розробнику програми;
- необхідно бути обережними щодо відвідування невідомих веб-сайтів, які можуть приховано завантажувати шкідливе програмне забезпечення на ваш пристрій;
- використовуйте захищені версії (https) веб-сайтів, коли ви маєте такий варіант;
- використовуйте ті самі запобіжні заходи, коли читаєте на своєму телефоні чи планшеті, а також на своєму комп'ютері (не відкривайте вкладення), і пам'ятайте, що текстові повідомлення SMS також можуть передавати шкідливе програмне забезпечення;
- якщо ви користуєтеся мобільним зв'язком для використання свого ноутбука чи планшета для підключення передачі даних 3G / 4G на своєму телефоні, не підключайтесь до точки доступу та обов'язково використовуйте WPA2, щоб захистити свою мережу Wi-Fi.

5. ***Планування особистого відновлення пошкоджень.*** Це означає, що ви можете дистанційно відстежувати, блокувати та / або видаляти дані на своїх мобільних пристроях, вибираючи безпечне та надійне програмне забезпечення.

Відповідно освітні установи та особисто вчителі мають розумітися на захисті, як своїх персональних даних, так і даних учнів та їх батьків, мають дотримуватися різних правил захисту даних. Так освітяни мають знати про законодавчі акти щодо захисту персональних даних; бажано офіційно укладати договір з постачальником обраного, для роботи хмарного сервісу; перевіряти в якій державі знаходиться провайдер та в яких місцях розташовані сервери; перевірити чи схвалене держорганами освіти, використання відповідного хмарного сервісу.

Варто зазначити що хмарні сховища мають безліч недоліків, але в той же час і не меншу кількість переваг. Потрібно чи ні довіряти свої персональні дані «хмарам» - це особисте питання для кожного користувача, але компанії, що надають дані послуги, з кожним роком намагаються збільшити безпеку своїх сховищ та зацікавлені в нових користувачах, а ті в свою чергу потребують конфіденційності, тому ступінь захисту персональних даних буде тільки збільшуватися.

Список використаних джерел

1. Bettermarks URL: https://de.bettermarks.com/ (дата звернення: 24.12.2018).
2. SchulCommSy Schleswig-Holstein URL: https://schulintern.sh.schulcommsy.de/ (дата звернення: 24.12.2018).
3. Five ways to protect yourself in a multi-device, multi-platform world URL: http://www.techrepublic.com/blog/security/five-ways-to-protect-yourself-in-a-multi-device-multi-platform-world/8233 (дата звернення: 24.12.2018).
4. Wie schützt man sich bei der Nutzung von Cloud-Diensten? URL: https://sicherheitskultur.at/Cloud_Security.htm (дата звернення: 24.12.2018).
5. Cloud Security Alliance URL: https://www.networkworld.com/article/3042610/security/the-dirty-dozen-12-cloud-security-threats.html (дата звернення: 24.12.2018).

Матеріал підготувала: Кравчина О.Є.наук.співр.

Адреса: Україна, 04060, м. Київ, вул. Максима Берлинського, 9
тел./факс: (044) 440–96–27
http:// http://iitlt.gov.ua/ ***e-mail:*** **comparative.iitzn@gmail.com**