DOI https://doi.org/10.36059/978-966-397-493-4-121

КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ХМАРНИХ ДАНИХ: ПРОБЛЕМИ КВАЛІФІКАЦІЇ

Діна ДРИЖАКОВА
аспірантка кафедри кримінально-правової політики та кримінального права
Київського національного університету імені Тараса Шевченка
м. Київ, Україна

У цифрову епоху хмарні технології стали невід'ємною частиною нашого життя, забезпечуючи зручне зберігання та обробку даних.

Хмарні системи дозволяють зберігання, обробку та використання даних на дистанційно розташованих комп'ютерах з доступом через Інтернет. Це відносно недорогий та зручний спосіб зберігання інформації, з мінімальними витратами для компаній і бізнесу.

Перше комерційне сховище з'явилося в 1994 році (PersonaLink Services network від AT&T), із того часу при використанні хмарного сховища інформація зберігається у зовнішнього постачальника послуг, наприклад, корпорації Майкрософт. Такий постачальник встановлює і обслуговує все апаратне і програмне забезпечення, а споживач отримує доступ до цих служб і керує своїм обліковим записом в Інтернеті[1].

Однак, зростання популярності хмарних послуг супроводжується збільшенням ризиків несанкціонованого доступу до хмарних даних, що становить серйозну загрозу для інформаційної безпеки. Кримінально-правова характеристика цього злочину має ряд особливостей, які ускладнюють його кваліфікацію та вимагають детального аналізу.

Закон України «Про хмарні послуги» (від 17.02.2022 р. № 2075-IX) визначає, що «технологія хмарних обчислень – технологія забезпечення дистанційного доступу на вимогу користувача до хмарної інфраструктури через електронні комунікаційні мережі»[2].

Хмарні обчислення представляють інформаційно-технологічну модель забезпечення повсюдного, ефективного та зручного доступу з використанням мережі Інтернет до загального набору обчислювальних ресурсів (хмари), пристроїв зберігання даних, додатків і сервісів, які можуть бути оперативно надані та/або звільнені від навантаження з мінімальними експлуатаційними витратами.

[1] Войнов М. Зберігання даних у хмарному сховищі: що робити у разі витоку конфіденційної інформації? // https://www.helsinki.org.ua/articles/zberihannia-danykh-u-khmarnomu-skhovyshchi-shcho-robyty-u-razi-vytoku-konfidentsiynoi-informatsii/

[2] Закон України «Про хмарні послуги» // https://zakon.rada.gov.ua/laws/show/2075-20#Text

Значний крок у розвитку правового регулювання використання технології хмарних сховищ інформації є вказівка на використання мережі Інтернет – це надання послуги у мережі Інтернет.

У науковій літературі розглядають хмарне сховище як модель онлайн-сховища, в якому дані зберігаються на численних розподілених у мережі серверах, що надаються в користування клієнтам. Хмарні сховища надають ІТ– компанії, які на легальній основі пропонують місце у центрі обробки даних для зберігання інформації, але не контролюють її.

Вчені розглядають правовідносини використання хмарного сховища інформації як оренди обчислювальної потужності центру обробки даних, підкреслюючи його значимість, оскільки там зберігається інформація, завантажена користувачем. Так, І. Шевчук та Б. Депутат вважають, що концепція технології хмарного сховища інформації полягає в наданні кінцевим користувачам віддаленого динамічного доступу до послуг, обчислювальних ресурсів та додатків через Інтернет[3]. [3]

Водночас А.Досенко розглядає хмарне сховище інформації як базу даних, що діє в режимі онлайн, при регулюванні якої завжди присутні питання транскордонних взаємодій[4]. [1]

Дане визначення є одним із найбільш точних, оскільки передає особливості регулювання хмарного сховища як бази даних та враховує можливість наявності іноземного елемента. Використання бази даних у більшості випадків можливе на підставі ліцензійного договору, де зберігання інформації (відомостей та/або даних) є ключовою функцією.

Програма хмарного сховища є системоутворюючою щодо інших сервісів, що мають функції обробки інформації. Хмарні сховища вже настільки розвинені, що поділяються на певні види, які визначені у Законі України «Про хмарні послуги» (Закон України «Про хмарні послуги») – приватна, колективна, публічна, гібридна.

На сьогодні існують деякі загрози для хмарних сховищ:

1. Міжмережеві атаки (Intercloud Attacks): Міжмережеві атаки являють собою загрози безпеці, які спрямовані на хмарні сервіси через їхню внутрішню інфраструктуру або пов’язані мережі. Ці атаки можуть мати різні форми та цілі, і вони підкреслюють необхідність посилення безпеки хмарних середовищ.

Види міжмережевих атак:

Сніффер-атаки – це крадіжки даних, спричинені перехопленням мережевого трафіку за допомогою сніфферів пакетів, які можуть незаконно отримати доступ до незашифрованих даних і прочитати їх.

[3] Ірина Шевчук, Богдан Депутат. ЕКОНОМІЧНИЙ АСПЕКТ ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ ТА БІЗНЕС-СТРУКТУР. Економіка та суспільство, (31)

[4] Досенко А. К. ХМАРНІ ТЕХНОЛОГІЇ:ПРИКЛАДНІ ТЕХНОЛОГІЇ СУЧАСНИХ ПЛАТФОРМ. // Прикладні соціально-комунікаційні технології . Том 33 (72) No 1 Ч. 3 2022.

Пакети даних перехоплюються, коли вони проходять через комп'ютерну мережу. Сніффери пакетів – це пристрої або носії інформації, які використовуються для здійснення сніффер-атаки та перехоплення мережевих пакетів даних. Їх називають аналізаторами мережевих протоколів. Якщо пакети не зашифровані за допомогою надійного мережевого захисту, хакери зможуть викрасти дані і отримати до них доступ. Існують різні аналізатори пакетів, такі як Wireshark, Dsniff, Etherpeek тощо.

Спуфінг – це акт маскування комунікації або ідентичності таким чином, щоб створити враження, що вона пов'язана з довіреним, авторизованим джерелом. Спуфінг-атаки можуть набувати різних форм, від звичайних підробок електронної пошти, які використовуються у фішингових кампаніях, до підробок ідентифікаторів абонентів, які часто використовуються для шахрайства. Зловмисники також можуть націлюватися на більш технічні елементи мережі організації, такі як IP-адреса, сервер системи доменних імен (DNS) або служба протоколу дозволу адрес (ARP), в рамках підміни.

Атаки за допомогою SQL-ін'єкцій полягають у вставці або «впровадженні» SQL-запиту через вхідні дані від клієнта до програми. Успішний експлойт SQL-ін'єкції може зчитувати конфіденційні дані з бази даних, модифікувати дані бази даних (вставляти/оновлювати/видаляти), виконувати операції адміністрування бази даних (наприклад, вимикати СУБД), відновлювати вміст певного файлу, присутнього у файловій системі СУБД, а в деяких випадках – віддавати команди операційній системі. Атаки типу SQL-ін'єкція – це різновид ін'єкційних атак, в яких команди SQL вводяться у вхідні дані для того, щоб вплинути на виконання попередньо визначених команд SQL.

2.DDoS-атаки (Distributed Denial of Service): DDoS-атаки являють собою форму кібератак, під час якої безліч комп'ютерів або пристроїв використовують для одночасного нападу на цільовий ресурс, перевантажуючи його і роблячи недоступним для легітимних користувачів. Ось кілька ключових аспектів DDoS– атак:

3. Дослідження слабких місць (Cloud Service Exploitation): Хмарні сховища надають безліч переваг, але вони також схильні до різних загроз безпеці. Дослідження слабких місць у безпеці хмарних сховищ може виявити вразливості, які можуть бути використані зловмисниками. Ось кілька типових загроз із дослідженням слабких місць:

1) Незадовільне управління доступом:

- Слабкі облікові записи: Використання слабких паролів або недостатнє управління обліковими записами може призвести до несанкціонованого доступу до хмарних даних.
- Відсутність багатофакторної автентифікації: Якщо ввімкнено тільки однофакторну автентифікацію, це може зробити облікові записи більш уразливими.

2) Необґрунтований розподіл прав доступу:

• Привілеї за замовчуванням: Деякі хмарні сховища можуть надавати зайві привілеї за замовчуванням, що збільшує ризик компрометації даних.

3) Недостатній захист даних:

• Відсутність шифрування: Якщо дані не шифруються в спокої або в процесі передачі, це може створити можливості для несанкціонованого доступу.

• Відсутність оновлень і патчів: Неоновлене програмне забезпечення може мати відомі вразливості, які зловмисники можуть використовувати.

4) Недостатній захист від загроз на рівні додатків:

• Дослідження слабких місць у коді: Зловмисники можуть шукати вразливості в коді застосунків, що працюють із хмарними даними.

• Несанкціоновані API-запити: Зловмисники можуть використовувати несанкціоновані API-запити для отримання доступу до даних.

5) Відсутність моніторингу та виявлення:

• Неактивні системи моніторингу: Якщо системи моніторингу неактивні або неправильно налаштовані, атаки можуть залишатися непоміченими.

• Недостатні журнали аудиту: Відсутність докладних журналів аудиту ускладнює виявлення аномальної активності.

6) Загрози, пов’язані з делегованим управлінням і передбачуваними довіреними відносинами:

• Компрометація довірених акаунтів: Якщо акаунти з довіреними правами доступу компрометовані, це може створити серйозні загрози безпеці.

• Недостатні контрольні заходи в делегованих відносинах: Відсутність суворих контрольних заходів у відносинах між хмарними постачальниками і клієнтами може стати джерелом загроз.

7) Недостатні засоби реагування та відновлення:

• Відсутність плану реагування на інциденти: Якщо організація не має чіткого плану з реагування на інциденти, це може ускладнити ефективне управління загрозами.

4. Проблеми кваліфікації

Кваліфікація несанкціонованого доступу до хмарних даних пов’язана з рядом проблем, зокрема:

Визначення поняття «хмарні дані»: Відсутність чіткого законодавчого визначення поняття «хмарні дані» ускладнює кваліфікацію злочину. Необхідно враховувати різні моделі хмарних послуг (IaaS, PaaS, SaaS) та особливості зберігання та обробки даних у кожній з них.

Юрисдикція: Хмарні сервіси можуть розташовуватися в різних юрисдикціях, що ускладнює визначення підслідності злочину.

Необхідно враховувати міжнародні договори та угоди про правову допомогу.

Доказування: Збір та аналіз цифрових доказів у хмарному середовищі вимагає спеціальних знань та навичок. Необхідно забезпечити належний захист цифрових доказів від спотворення або знищення.

Відповідальність хмарних провайдерів: Необхідно визначити межі відповідальності хмарних провайдерів за захист даних користувачів. Важливо враховувати умови договору про надання хмарних послуг.

Транскордонність: Хмарні злочини часто мають транскордонний характер, що ускладнює розслідування та притягнення до відповідальності.

Динамічність розвитку хмарних технологій: Швидкий розвиток хмарних технологій вимагає постійного оновлення законодавства та правозастосовчої практики.

5. Шляхи вирішення проблем кваліфікації

Для вирішення проблем кваліфікації несанкціонованого доступу до хмарних даних необхідно:

удосконалити законодавство, зокрема шляхом внесення змін до статті 361 КК України, уточнивши поняття «інформаційна система» та врахувавши сучасні технологічні реалії;

розробити та прийняти стратегію кібербезпеки України на період повоєнного відновлення;

імплементувати міжнародні стандарти у сфері кібербезпеки;

підвищити кваліфікацію правоохоронних органів, суддів та прокурорів у сфері кібербезпеки;

розвивати міжнародну співпрацю у сфері боротьби з кіберзлочинністю;

підвищувати рівень обізнаності громадян щодо кібербезпеки та захисту персональних даних.

Висновки

Кримінально-правова кваліфікація несанкціонованого доступу до хмарних даних є складною проблемою, що потребує подальшого дослідження та вдосконалення законодавства. Необхідно забезпечити ефективну співпрацю між правоохоронними органами, хмарними провайдерами та міжнародними організаціями для протидії цьому виду злочину.