УДК 004.056.5:004.57.2
DOI: 10.31673/2412-9070.2022.040916

Л. В. ДАКОВА[1], канд. техн. наук, доцент;
С. Ю. ДАКОВ[2], канд. техн. наук;
Н. В. БЛАЖЕННИЙ[1], ст. викладач;
Д. О. СТАДНИК[1], магістр;
І. І. ПАРХОМЕНКО[2], канд. техн. наук, доцент,
[1] Державний університет телекомунікацій, Київ
[2] Київський національний університет імені Тараса Шевченка

МЕХАНІЗМИ БЕЗПЕКИ В ХМАРНОМУ СЕРЕДОВИЩІ НА БАЗІ МІЖНАРОДНИХ СТАНДАРТІВ

Удосконалено стандартизований функційний підхід до процедури оцінювання відповідності, ґрунтуючись на специфіці функціонування хмарних технологій. Здійснено огляд сучасних фреймворків, які використовуються для оцінювання та сертифікації надавачів хмарних послуг (НХП), щодо відповідності вимогам загальновизнаних стандартів безпеки.

Запропоновані рівні гарантій передбачають розроблення особливих вимог стосовно забезпечення безпеки інформаційних систем НХП відповідно до класифікації критичності систем і даних потенційних споживачів хмарних послуг.

Керуючись нормативними актами, нормами міжнародних стандартів і вже розглянутими національними схемами з оцінювання кібербезпеки хмарних продуктів, сервісів і послуг, сформулювано узагальнений список вимог до безпеки надавачів хмарних послуг, який охоплює всі необхідні умови та відповідає запропонованим рівням гарантій.

Здійснено оцінювання відповідності стандартам безпеки, яке є відправною точкою для визначення політики інформаційної безпеки та боротьби із загрозами, що притаманні хмарним сервісам.

Запропоновано розподіл на три рівні гарантій безпеки, яким має відповідати НХП під час оцінювання відповідності залежно від бізнес-потреб користувачів і критичності даних, котрі обробляє та зберігає хмарна інформаційна система. Розроблено узагальнену схему вимог безпеки до НХП, побудовану на основі загальновідомих фреймворків, яка бере до уваги різнорівневий підхід до гарантій безпеки, розподілену відповідальність за дотримання перелічених вимог залежно від моделі функціонування і визначає компоненти архітектури хмари, що є чутливими до тих чи інших умов.

У статті поєднано всі найкращі стандарти Сполучених Штатів Америки та Європейського Союзу, а також найкращі практики безпеки для використання хмарного середовища, яке вважається найнебезпечнішим з погляду інформаційної безпеки, але зручним для використання.

Ключові слова: надавач послуг; хмара; хмарна інфраструктура; мережа.

ВСТУП

Надавачі хмарних послуг **(НХП)** мають спеціальні сертифікати відповідності та звіти аудитів безпеки, які вони повинні пройти для забезпечення безпеки інформаційних систем, але саме організація — користувач хмарних послуг бере на себе зобов'язання щодо пошуку правильного постачальника, ґрунтуючись на вимогах кібербезпеки бізнес-індустрії, та залишається власником своїх даних, незважаючи на фізичну відсутність контролю безпеки у хмарі.

Більшість постачальників хмарних послуг несуть спільну відповідальність з користувачами, тобто розрізняють «безпеку хмари» (відповідальність постачальника хмарних послуг) та «безпеку в хмарі» (відповідальність користувача). Це означає, що постачальник обіцяє підтримувати безпеку інфраструктури та пропонує надійні інструменти безпеки, але відповідальність за налаштування та захист своїх даних, підтримання постійного регуляторного контролю лежить на клієнтові і, зрештою, повна вага щодо захисту інформації покладається саме на користувача хмарних послуг. Оцінювання відповідності стандартам безпеки може стати початком для визначення своєї політики інформаційної безпеки та боротьби із загрозами, притаманними хмарним сервісам.

ОСНОВНА ЧАСТИНА

Сьогодні в більшості джерел щодо хмарних технологій не розглядаються всі наявні стандарти. Наприклад, у джерелах [2–5] розкрито лише основні положення, визначені в стандартах 17000, 27000, 19000 тощо. Але вивчати потрібно весь спектр стандартів у сукупності з найкращими практиками.

Хмарне середовище — це найбільш сучасна і гнучка система керування ІТ-процесами будь-якої компанії, не йдеться навіть про розмір і прибуток, бо хмарні сервіси можна розширяти або навпаки зменшувати згідно з умовами [6; 7].

Проведення регулярних процедур оцінювання відповідності допомагає дістати більш повне розуміння своїх онлайн-операцій та архітектури,

перевірити, чи ефективно відбувається захист даних користувачів від усіх потенційних векторів і методів атак, сприяє оптимізації необхідних ресурсів, визначенню потреб у навчанні співробітників, розробленню планів аварійного відновлення і реагування на інциденти, а також установленню потенційних ризиків безпеки і побудові планів їх усунення [8; 9].

Тому цю статтю спрямовано на охоплення більшості стандартів і найкращих практик із безпеки в розвинених країнах, компаніях та корпораціях, які вже використовують хмарні обчислення, що надасть можливість читачу детальніше оцінити ризики переведення інформаційної системи в хмарне середовище.

Процедура оцінювання відповідності надавачів хмарних послуг

Загальний функційний підхід, описаний ДСТУ ISO/IEC 17000:2020, може бути застосовний для проведення оцінювання відповідності надавачів хмарних послуг [10; 11].

Для підвищення ефективності цієї процедури варто зважати на деякі нюанси, що стосуються здебільшого ринку хмарних обчислень.

Деталізовану та доповнену схематичну версію функційного підходу до оцінювання відповідності надавачів хмарних послуг зображено на рис. 1.

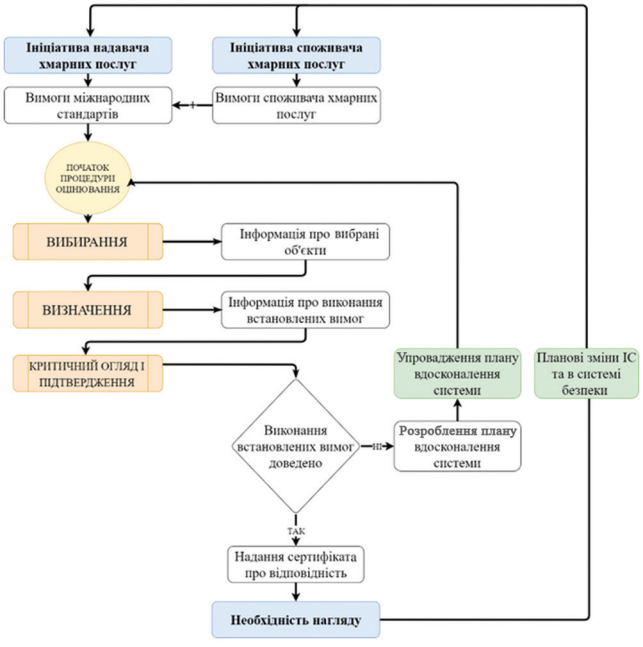

Рис. 1. Розширений функційний підхід до оцінювання відповідності надавачів хмарних послуг

Ключовою особливістю інформаційних технологій, порівняно з іншими галузями діяльності, є дуже висока динамічність розвитку, тому функція «Необхідність нагляду» стає критично важливою в цій сфері — надавачі хмарних послуг потребують систематичного проведення контролю безпеки ІС і підтвердження відповідності вимогам як міжнародних стандартів, нормативних актів, законодавства України, так і контрактних умов.

Окрім цього, потрібно передбачити функцію «Вдосконалення системи», яка описуватиме зміни фізичної, логічної та організаційної структури організації для того, щоб полегшити подальші процедури оцінювання відповідності.

Схема також окреслює два основних джерела ініціалізації проведення процедури оцінювання відповідності — це може бути як ініціатива НХП, так і запит потенційних користувачів хмарних послуг, які визначили пакет стандартів, потрібних для ведення бізнесу, та наклали власні вимоги до безпеки інформаційних систем.

Надання сертифіката про відповідність має свої особливості та потребує окремо визначених процедур керування. Головними умовами видачі сертифіката є успішне оцінювання хмарного сервісу та перевірка результатів цього оцінювання, яке має виконуватись незалежно і охоплювати огляд усіх наданих звітів, щоб переконатися в тому, що висновки узгоджуються з наданими доказами та правильно застосовано прийняті критерії та методи оцінювання. Орган, відповідальний за сертифікацію НХП, визначає термін дії сертифіката, який не перевищує трьох років. Протягом цього терміну необхідні періодичні повторні оцінювання, щоб гарантувати постійне виконання провайдером установлених вимог. Відповідно до результатів оцінювання сертифікат може набувати різних статусів. Наприклад, статус «Новий» (коли НХП уперше підтвердив свою відповідність), «Оновлений» (для відображення деяких змін), «Зупинений» (до виправлення невідповідностей), «Поновлений» (після підтвердження усунення виявлених недоліків), «Продовжений» (затверджений без змін після закінчення терміну дії), «Відкликаний» (через незадоволення вимог безпеки після трьох місяців від призупинення дії сертифіката).

Аналіз сучасних специфікацій

Існує кілька загальноприйнятих схем, що містять загальний перелік вимог до надавача хмарних послуг та методи проведення процедур їх сертифікації.

Зокрема мінімальною вимогою на етапі вибору постачальників хмарних послуг є відповідність стандарту *Service Organization Control 2* **(SOC 2)**. Це процедура аудиту, розроблена AICPA, яка гарантує, що постачальники послуг безпечно керують даними користувачів для захисту інтересів організації та конфіденційності її клієнтів. Звіт про аудит SOC 2 демонструє, що НХП дотримується політики, процедур та засобів контролю, які відповідають п'ятьом принципам довіри: безпеці, доступності, цілісності оброблення, конфіденційності та приватності.

Існує два типи звітів SOC 2:

• **тип I** описує системи постачальника та визначає, чи задовольняє їхня конструкція відповідні принципи довіри;

• **тип II** детально описує експлуатаційну ефективність цих систем.

На відміну від PCI DSS, який має дуже жорсткі вимоги, звіти SOC 2 унікальні для кожної організації. Згідно з певною діловою практикою кожен розробляє власні засоби контролю, щоб відповідати принципам довіри [8].

Найбільш відомою схемою сертифікації є *Cloud Controls Matrix* **(CCM)**, розроблена *Cloud Security Alliance* **(CSA)**. Місія цієї організації полягає в тому, щоб «сприяти використанню найкращих практик забезпечення безпеки в хмарних обчисленнях». Саме CSA створила першу в галузі сертифікацію хмарної безпеки в 2010 році, яка нині є загальновизнаною у світі [9].

CCM — це структура керування кібербезпекою для хмарних обчислень, яка відповідає найкращим практикам CSA та вважається фактичним стандартом хмарної безпеки й конфіденційності. Ця матриця контролів містить 16 доменів, які охоплюють усі ключові аспекти хмарних технологій. Кожен домен розбитий на 133 контрольні цілі. CCM слугує керівництвом, щоб допомогти організаціям визначити спільні обов'язки між надавачем та користувачами хмарних послуг під час упровадження контролю безпеки. Для кожного елемента керування він також визначає, які хмарні архітектурні й організаційні моделі стека й хмарних сервісів застосовні.

Для спрощення здійснення оцінювання відповідності CSA розробила супровідний Опитувальник ініціативи з оцінювання консенсусу (CAIQ), який містить набір запитань «так чи ні» на основі засобів контролю безпеки в CCM.

Головною європейською схемою для оцінювання відповідності НХП є Схема сертифікації кібербезпеки Європейського Союзу для хмарних послуг (далі — EUCS) [10]. Схема ґрунтується на багатьох різних джерелах, першим з яких є звіт робочої групи *Cloud Service Provider Certification* (CSP-CERT), що був репрезентований у 2019 році та надав базове підґрунтя, на основі якого було розроблено EUCS. Вимоги безпеки, визначені у схемі, переважно дотримуються стандартів серії ISO27000, німецької схеми BSI C5, SecNumCloud, звіту CSP-CERT та принципів інших схем, що використовуються в Європі, а процедуру оцінювання відповідності засновано на стандарті ISO/IEC 17065.

Рівень гарантій повинен бути співмірним із рівнем ризику, пов'язаним із передбачуваним використанням продуктів, послуг або порцесів, які пропонує хмарна система. А отже, вимоги безпеки, що задовольняють кожний рівень гарантії, мають бути задокументовані у відповідній схемі сертифікації інформаційної безпеки, включно з відповідною функцією безпеки та відповідною суворістю і глибиною оцінювання, яке має пройти надавач хмарних послуг.

Оптимальним варіантом є розподіл вимог, запропонований EUCSA, який передбачає три рівні гарантій безпеки: *базовий*, *середній* та *високий*.

Запропоновані рівні гарантій передбачають розроблення особливих вимог до забезпечення безпеки інформаційних систем НХП відповідно до класифікації критичності систем і даних потенційних споживачів хмарних послуг. У такому разі оцінювання відповідності вимогам демонструє користувачам, наскільки високими є гарантії інформаційної безпеки під час користування послугами надавачів хмари.

З огляду на нормативні акти, норми міжнародних стандартів і вже розглянуті національні схеми з оцінювання кібербезпеки хмарних продуктів, сервісів і послуг [10; 11] можна сформулювати узагальнений список вимог до безпеки надавачів хмарних послуг, який охоплюватиме всі необхідні умови та відповідатиме запропонованим рівням гарантій. Усі аспекти вимог безпеки слід розглядати з погляду функціональних, фізичних та бізнес-вимог. Крім того, вимоги безпеки мають випливати з цілей безпеки і/або організаційних цілей і нормативних вимог.

Керування активами організації

Активи містять у собі фізичні та віртуальні об'єкти, потрібні для інформаційної безпеки хмарного сервісу під час створення, оброблення, зберігання, передавання, видалення або знищення інформації в зоні відповідальності НХП. До їх переліку належать, наприклад, брандмауери, балансувальники навантаження, вебсервери застосунків і сервери баз даних. Особливим активом організації вважаються також людські ресурси, які потребують особливої уваги, адже вони є критичним елементом інформаційної безпеки інформаційної системи.

• ***Керування активами***. НХП повинен визначити власні активи організації і забезпечити належний рівень їх захисту протягом усього життєвого циклу. Він охоплює етапи затвердження придбання, уведення в експлуатацію, виведення з експлуатації та утилізацію обладнання. Водночас варто брати до уваги інвентаризацію та класифікацію активів, безпечне налаштування механізмів оброблення помилок, реєстрацію, шифрування, автентифікацію та авторизацію, обмеження використання ПЗ або використання сервісів, захист від шкідливих програм, віддалену дезактивацію або блокування, фізичне доставляння і транспорту-

вання, роботу з уразливостями та повне видалення даних після виведення з експлуатації.

• ***Керування персоналом.*** Навмисні та ненавмисні дії працівників залишаються найбільш поширеним джерелом загроз витоку даних. Для уникнення ризиків, пов'язаних із інсайдерами організації, кожен з учасників відносин у сфері хмарних обчислень повинен суворо дотримуватись правил для співробітників, установлених політикою безпеки організації.

Організаціям, які допускають можливість дистанційної роботи, слід сформулювати політику, яка визначатиме умови та обмеження роботи поза звичайним офісом. Захищені комунікації в такому разі мають зважати на необхідність авторизованого віддаленого доступу до внутрішніх систем організації, запобігаючи обробленню та зберіганню інформації на приватному обладнанні, забезпечуючи конфіденційність інформації під час передавання по лінії зв'язку і передбачаючи можливість відкликання повноважень, прав доступу та повернення активів організації.

Критичні елементи керування безпекою

Рекомендовано такий перелік вимог до керування ризиками, змінами, ланцюгами постачань, неперервністю бізнесу та забезпеченням сумісності і портативності хмари відповідно до рівня гарантій у процесі оцінювання відповідності НХП.

• ***Керування ризиками.*** Надавач хмарних послуг зобов'язаний створити офіційну, задокументовану та спонсоровану керівництвом програму керування ризиками підприємства, яка охоплює політику та процедури для ідентифікації, оцінювання, володіння, оброблення та прийняття ризиків хмарної безпеки й конфіденційності.

Водночас керівництво має сприяти координації між організаційними структурами, відповідальними за різні аспекти хмарної безпеки та ризиків конфіденційності і, за потреби, переглядати програму, щоб усунути зміни ландшафту загроз та істотні зміни в організації.

• ***Керування змінами.*** Ринок інформаційних технологій є надзвичайно динамічним, тому зміни — невід'ємна складова хмарних обчислень, що зумовлює додаткові ризики стосовно безпеки функціонування хмарних систем. Саме тому НХП мають дотримуватись процедур керування ризиками, пов'язаних зі змінами в активах організації, включно з програмами, системами, інфраструктурою, конфігурацією систем тощо, незалежно від того, керування активами здійснюється внутрішньо чи зовнішньо.

При цьому потрібно передбачити процедуру керування винятками, зокрема під час виникнення надзвичайних ситуацій, і визначити процедуру для активного відновлення змін до попередньо відомого задовільного стану в разі помилок або проблем безпеки.

• ***Керування ланцюгами постачань.*** Характерною особливістю хмарних технологій є модель спільної відповідальності за безпеку кожного з учасників хмарних сервісів, включно з третіми сторонами — постачальниками продуктів і послуг.

Важливо задокументувати стратегії, що забезпечуватимуть мінімальне порушення бізнесу в разі припинення відносин із постачальниками. Стратегії виходу мають бути узгодженими з оперативними планами неперервності бізнесу та охоплювати аналіз потенційних витрат, впливу, ресурсів і термінів переходу до альтернативного постачальника.

• ***Керування неперервністю бізнесу.*** Однією з найбільших переваг, які пропонуються користувачам хмарних обчислень, є гарантія неперервності ведення бізнесу за будь-яких умов, тому від надавачів послуг вимагається визначити вплив збоїв хмарних систем для розроблення стратегій керування неперервністю бізнесу та операційної стійкості.

План керування неперервністю бізнесу передбачає створення резервних копій даних, що зберігаються в хмарі, забезпечення їх конфіденційності, цілісності і доступності, а також перевірку відновлення даних із створеної резервної копії.

Окрім цього, хмара має підтримувати план реагування на катастрофи для відновлення після стихійних і техногенних катастроф. План аварійного відновлення зобов'язує хмарних провайдерів доповнювати критичне для бізнесу обладнання резервним устаткуванням, розташованим на розумній мінімальній відстані відповідно до застосовних галузевих стандартів або в межах угод про рівень обслуговування SLA.

• ***Сумісність і портативність.*** Користувачі хмарних сервісів повинні мати можливість доступу до хмари через інші хмарні сервіси або інформаційні системи клієнтів, а також отримати збережені дані після закінчення договірних відносин та безпечно видалити їх із хмари НХП.

Угода з користувачем має містити положення, що визначають доступ користувачів хмарних технологій у разі розірвання договору, які будуть передбачати формат, обсяг даних, тривалість часу, протягом якого вони будуть зберігатися, та політику видалення даних. Видалення даних користувачів має охоплювати метадані, дані, що зберігаються в резервних копіях, а також технічні дані, що стосуються клієнта (наприклад, каталоги, сертифікати, конфігурації доступу).

Організація повинна використовувати тестування безпеки політики і процедур сумісності та портативності. Докази проведених і запланованих

тестів безпеки для всіх систем сумісності та портативності мають надаватися відповідно до контрактних угод або на запит користувачів.

Безпека хмарної інфраструктури та віртуального середовища

Інфраструктура хмарних провайдерів викликає найбільшу недовіру у користувачів, адже відповідальність за її безпеку лежить тільки на НХП.

Надавачам хмарних послуг рекомендовано впроваджувати захист від зловмисного програмного забезпечення, моніторинг цілісності файлів і журналювання, а також використовувати довіру на основі апаратного забезпечення до модулів віртуальної надійної платформи (vTPM). За можливості, організації повинні використовувати мінімалістичні, специфічні для контейнера операційні системи (ОС) із вимкненими всіма іншими службами та функціональними можливостями, а також із файловими системами лише для читання та іншими методами посилення, які використовуються для зменшення поверхонь атак:

- хости, які запускають контейнери, мають запускати лише контейнери, а не інші програми, такі як вебсервери або бази даних, поза контейнерами;
- хости, які запускають контейнери, повинні постійно перевірятися на наявність уразливостей і швидко оновлюватися;
- основна ОС не повинна запускати непотрібні системні служби;
- доступ до хоста контейнера має базуватися на принципах необхідності знати та найменших привілеїв;
- для контейнерів слід використовувати моніторинг цілісності файлів і виявлення вторгнень на хост.

Однією з найважливіших вимог є безпечне проєктування, розроблення, розгортання та налаштування застосунків та інфраструктури в такий спосіб, щоб доступ користувачів та доступ всередині організації був належно сегментований та відокремлений, контрольований та обмежений від інших орендарів. Можливі визначення сегментації мають варіюватися від *повної ізоляції* до *часткового логічного поділу критично важливих для бізнесу активів і/або персональних даних/конфіденційних даних користувача та сеансів*. Робочі навантаження між орендарями та бізнес-напрямками мають бути сегментовані відповідно до концепції найменших привілеїв, щоб зменшити поверхню атаки. До того ж для робочих навантажень слід використовувати теги робочого навантаження, імена ресурсів та ідентифікацію.

Крім цього, мають застосовуватись безпечні та зашифровані канали зв'язку під час міграції серверів, служб, застосунків або даних у хмарні середовища. Такі канали мають послуговуватись лише сучасними та затвердженими протоколами. Безпечний зв'язок під час міграції фізичних серверів, служб, програм або даних у віртуалізоване середовище може використовувати комбінацію вимог до конфіденційності, цілісності, автентифікації, автентифікації джерела, авторизації та невідмовності.

Уразливості у фізичному середовищі також несуть небезпеку у ***віртуальному середовищі***. Недоліки конфігурації та недоліки в програмах, брандмауерах або мережах залишаються вразливими до експлойтів, спуфінгу, атак із відмови доступу тощо, тому методи глибокого захисту повинні бути застосовні як для фізичного, так і для логічного й адміністративного керування.

- ***Безпека ЦОД***. Фізичний захист інфраструктури може здатись трюїстичним, проте він залишається одним із критично важливих, зокрема й для технологій хмарних обчислень.

Будь-які фізичні та логічні активи мають бути класифіковані, каталогізовані та відстежувані на основі організаційного бізнес-ризику. Персонал ЦОД повинен використовувати рішення, яке дає змогу відстежувати інвентаризацію та керувати фізичним розташуванням серверів та інших активів ЦОД, виводячи паперові та ручні процеси. Розміщене рішення з відстеження активів для серверів, комутаторів, відстеження активів ЦОД зазвичай використовує технології пасивної радіочастотної ідентифікації, глобальної системи позиціонування і/або технології Bluetooth Low Energy.

Надавач хмарних послуг має забезпечити захист інформації в мережах за допомогою спеціальних технічних засобів для виявлення та реагування на мережні атаки, а також організаційних заходів. Зокрема, потрібно задокументувати вимоги до логічного і фізичного розподілення мережі на зони безпеки, дозволені комунікаційні відносини, мережні та прикладні протоколи, особливості адміністративних мереж та міжмережне спілкування. Для здійснення моніторингу відповідності цим вимогам обов'язковим є регулярне оновлення топологічних схем мережі та переліку використовуваного мережного обладнання.

- ***Керування безпекою кінцевих точок***. Кінцеві точки — одне з найвразливіших місць інформаційної системи. Тож і технології хмарної інфраструктури не є винятком. Надавач хмарних послуг має підтримувати політику безпечного користування кінцевими точками.

Там, де це можливо, організації також повинні вимкнути порти, заборонити використання записувальних пристроїв, перевіряти змінні носії, вкладені файли електронної пошти та вебтрафік.

• ***Безпека хмарних застосунків.*** Надавачі послуг зобов'язані ухвалити і підтримувати політики та процедури безпеки застосунків для відповідного планування й організації можливостей безпеки хмарних сервісів відповідно до встановлених політик безпеки і галузевих стандартів.

Хмарні провайдери повинні сприяти використанню встановленого життєвого циклу розроблення програмного забезпечення, аби гарантувати, що безпека інтегрована в продукт із моменту його створення, а наявні ризики було усунено на початкових етапах розроблення. Зокрема, це проєктування, перегляд коду, дизайну, навчання безпечному кодуванню, стратегії тестування (функціонального, регресійного, безпекового тощо), тестування вразливостей, безпечного розгортання, керування змінами та процесами завершення існування застосунку.

Прикладами технічних показників під час проведення тестування можуть бути підрахунок уразливостей за слабкими місцями/серйозністю/джерелами виявлення (огляд дизайну, огляд коду, статичне і динамічне тестування безпеки, тестування на проникнення або пошук уразливостей), середній час розв'язання проблеми або підрахунок перевищення цілей рівня послуг із відновлення.

Ці задокументовані принципи мають стосуватись не тільки застосунків, створених власними силами, а й від зовнішніх постачальників.

• ***Безпека даних.*** Політика та процедури для класифікації, захисту й оброблення даних протягом усього їхнього життєвого циклу є необхідною вимогою відповідно до всіх застосовних законів, правил і стандартів.

Політика безпеки даних повинна передбачати надійні методи для безпечного видалення даних без можливості їх відновлення, сувору інвентаризацію даних та їх потоків, щоб визначити власників інформації та їх обов'язки, які дані обробляються, де фізично зберігаються та обробляються, де розміщено резервні копії і куди їх передають.

Керування ідентифікацією та доступом

Далі розглянемо узагальнені ключові вимоги до організації керування ідентифікацією та доступом відповідно до рівня оцінювання.

Надавачі хмарних послуг повинні підтримувати політику та процедури для керування ідентифікацією та доступом до інформації, а також засобів її оброблення. Вона охоплює контроль доступу до реєстрації, керування та видалення цифрових ідентифікаційних даних, надійний парольний захист, інформацію про системні унікальні ідентифікатори і рівні доступу, застосовуючи політику контролю доступу на основі ролей та розподілу обов'язків.

Користувачі, які мають ОЗ з привілейованими правами доступу, потребують особливого контролю, тому варто передбачити процеси, процедури та технічні заходи щодо розподілу ролей привілейованого доступу на обмежений період часу, аби адміністративний доступ до даних, можливості шифрування та керування ключами і можливості ведення журналів були чіткими та розділеними.

Надавач хмарних послуг має також упровадити процедури та технічні заходи для багатофакторної автентифікації та політики єдиного входу. Для доступу до всіх середовищ, включно з невиробничими, потрібна надійна автентифікація (для персоналу це багатофакторна автентифікація, а для користувачів, які не є людьми — автентифікація за допомогою криптографічного механізму, який задовольняє вимоги безпеки).

Нарешті, весь доступ (особливо привілейований) слід реєструвати та відстежувати стосовно аномалій та несанкціонованого використання, а також пов'язувати із системами оповіщення відповідно до потреб за допомогою рішення для керування інформацією та подіями безпеки.

Криптографія та керування ключами

Криптографічна система захисту інформації — обов'язкова вимога до хмарних сервісів відповідно до законодавства України. Надавач хмарних послуг забезпечує криптографічний захист даних у стані спокою, які охоплюють бази даних, робочі станції кінцевих користувачів і файлові сервери, та в стані передавання (містить системні інтерфейси, загальнодоступні мережі та електронні повідомлення), із урахуванням класифікації даних і пов'язаних ризиків, використовуючи криптографічні бібліотеки та генератори випадкових чисел, сертифіковані за затвердженим стандартом.

Криптографія забезпечує захист даних: конфіденційність, цілісність, доступність та автентифікацію джерела. До того ж організації повинні мати можливість або шифрувати всю інформацію на пристроях зберігання (тобто повне шифрування диска), або шифрувати конкретні структури даних (наприклад, файли, записи чи поля).

Можливість керувати ключами може бути надано для користувачів хмарних сервісів, проте обсяг ключів, їх довжина, алгоритми шифрування і відповідальність за керування політикою, процедурами і процесами мають бути суворо задокументовані.

Операційна безпека

Існує перелік вимог, запропонованих для забезпечення керування загрозами та вразливостями, логування та моніторингу інцидентів безпеки, а також їх розслідування відповідно до запропонованого рівня гарантій під час оцінювання відповідності НХП.

Операційна безпека системи забезпечує належну та регулярну роботу, включно з відповідними заходами щодо планування та моніторингу потужностей хмарних сервісів, захисту від шкідливих програм, процесів логування та моніторингу, а також боротьби з уразливими місцями інформаційної системи, загрозами безпеки та розслідуванням виявлених інцидентів.

• ***Керування загрозами та вразливостями.*** Щоб захистити системи хмарних обчислень від експлуатації вразливостей зловмисником, потрібно запровадити політику керування загрозами та вразливостями (далі — TVM), а також процедури для виявлення, звітування і визначення пріоритетів усунення вразливостей, процедури для захисту від зловмисного програмного забезпечення на керованих активах, а також процедури та технічні заходи для забезпечення можливості як планового, так і екстреного реагування на вразливості на основі виявленого ризику. Потрібно передбачити регулярне оновлення засобів виявлення загроз на основі сигнатур та індикаторів компрометації — зазвичай щотижня, або навіть частіше.

Має бути впроваджено інтегровану систему TVM, яка зможе вести облік загроз та вразливостей, виявлених із часом, та результатів дій щодо їх пом'якшення. Інтегровану систему TVM слід застосовувати щодо пом'якшення всіх майбутніх ризиків, використовуючи попередній досвід заходів із пом'якшення, а також для складення графіку усунення виявлених уразливостей, його моніторингу і нагляду за залишковими ризиками.

• ***Логування та моніторинг.*** Організації, що використовують технології хмарних обчислень, повинні відстежувати пов'язані з безпекою події в застосунках та базовій інфраструктурі з подальшим упровадженням системи для генерування сповіщень відповідальним зацікавленим сторонам на основі таких подій та відповідних показників.

Організації мають упровадити процес своєчасного виявлення та звітування про збої критичних систем контролю безпеки за допомогою брандмауерів, систем виявлення вторгнень, систем запобігання вторгненням, моніторингу цілісності файлів, антивірусів, здійснення фізичного та механічного контролю доступу та механізмів реєстрації аудиту.

• ***Розслідування інцидентів.*** Надавач хмарних послуг зобов'язаний розробити план реагування на інциденти, який утворює так звану дорожню карту для оброблення інцидентів, пов'язаних із хмарними сервісами організації та продуктами і послугами, на які ці послуги покладаються. Ці плани мають застосовуватися незалежно від того, чи є ці залежності внутрішніми (наприклад, IT, операції, підтримання та юридичні), чи зовнішніми (постачальники, партнери, клієнти та інші треті сторони). План має бути надійним, своєчасним, узгодженим із планами організації неперервної діяльності та аварійного відновлення, тому потребує регулярного тестування й оновлення.

ВИСНОВКИ

Обґрунтовано потребу в оцінюванні відповідності вимогам НХП та розглянуто такі питання:

• удосконалено стандартизований функційний підхід до процедури оцінювання відповідності, ґрунтуючись на специфіці функціонування хмарних технологій;

• здійснено огляд сучасних фреймворків, які використовуються для оцінювання та сертифікації НХП щодо відповідності вимогам загальновизнаних стандартів безпеки;

• запропоновано розподіл на три рівні гарантій безпеки, яким має відповідати НХП у процесі оцінювання відповідності залежно від бізнес-потреб користувачів і критичності даних, які обробляє та зберігає хмарна інформаційна система;

• розроблено узагальнену схему вимог безпеки до НХП, побудовану на основі загальновідомих фреймворків, в якій взято до уваги різнорівневий підхід до гарантій безпеки, розподілену відповідальність за дотримання перерахованих вимог залежно від моделі функціонування, визначаючи компоненти архітектури хмари, котрі є чутливими до тих чи інших умов.

Список використаної літератури

1. ***Матриця*** *Cloud Controls i CAIQ v4 [Електронний ресурс] // CSA, 07.06.2021. URL:*

https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.

2. ***Про хмарні*** *послуги [Електронний ресурс]: Закон України від 17.02.2022 № 2075-IX. URL:*

https://zakon.rada.gov.ua/laws/show/2075-20#n69.

3. ***Жилін А., Дівіцький А., Козачок А.*** *Проблематика захисту інформаційних ресурсів при використанні хмарних технологій // Information Technology and Security. 2019. № 7. P. 171–182.*

4. ***The Security*** *Guidance for Critical Areas of Focus in Cloud Computing v4.0 [Електронний ресурс] // CSA, 07.26.2017. URL:*

https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf.

5. ***NIST*** *Special Publication 500-292, NIST Cloud Computing Reference Architecture [Електронний ресурс]. URL:*

https://bigdatawg.nist.gov/_uploadfiles/M0008_v1_7256814129.pdf.

6. ***ISO/IEC 27001.*** *Information technology — Security techniques — Information security management systems — Requirements [Електронний ресурс].*

URL:
https://www.iso.org/isoiec-27001-information-security.html.

7. ***ISO/IEC 27017.*** *Information technology - Security techniques - Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002 [Електронний ресурс]. URL:*
https://www.iso.org/standard/43757.html.

8. ***ISO/IEC 27002:2022.*** *Information security, cybersecurity and privacy protection — Information security controls [Електронний ресурс]. URL:*
https://www.iso.org/standard/75652.html.

9. ***Про технічні*** *регламенти та оцінку відповідності [Електронний ресурс]: Закон України від 19.02.2022 № 124-VIII. URL:*
https://zakon.rada.gov.ua/laws/show/124-19#Text.

10. ***SOC 2*** *Compliance [Електронний ресурс] // Imperva, 12.07.2021. URL:*
https://www.imperva.com/learn/data-security/soc-2-compliance/.

11. ***EUCS*** *– Cloud Services Scheme [Електронний ресурс] // ENISA, 22.12.2020. URL:*
https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.

L. Dakova, S. Dakov, N. Blazhennyi, D. Stadnik, I. Parkhomenko

SECURITY MECHANISMS IN THE CLOUD ENVIRONMENT BASED ON INTERNATIONAL STANDARDS

A standardized functional approach to the conformity assessment procedure has been improved, based on the specifics of the functioning of cloud technologies. A review of the existing frameworks, which are used for the evaluation and certification of the Cloud Service Provider (further to the CSP), in terms of compliance with the requirements of generally recognized security standards, was carried out.

The proposed levels of guarantees provide for the development of special requirements for ensuring the security of information systems of cloud service providers in accordance with the classification of criticality of systems and data of potential consumers of cloud services.

Guided by regulatory acts, norms of international standards and already considered national schemes for evaluating the cyber security of cloud products, services and services, a generalized list of requirements for the security of cloud service providers has been formulated, which covers all the necessary conditions and corresponds to the proposed levels of guarantees.

An assessment of compliance with security standards was carried out, which is the starting point for determining information security policy and combating threats inherent in cloud services.

The division into three levels of security guarantees, which should be met by the CSP when evaluating compliance, is proposed depending on the business needs of users and the criticality of the data processed and stored by the cloud information system.

A generalized scheme of security requirements for CSP has been developed, built on the basis of well-known frameworks, which takes into account a multi-level approach to security guarantees, distributed responsibility for compliance with the listed requirements depending on the functioning model and determines the components of the cloud architecture that are sensitive to certain conditions.

This article combines all the best standards of the United States and the European Union and the best security practices for using a cloud environment that is considered the most dangerous from the point of view of information security, but convenient to use.

Keywords: service provider; cloud; cloud infrastructure; network.