ЧАНИШЕВ РАШИД ІБРАГІМОВИЧ

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат юридичних наук, доцент

ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ЗБЕРІГАЄТЬСЯ У ЦЕНТРАХ ОБРОБКИ ДАНИХ

Військова агресія РФ проти України, що почалася 24 лютого 2022 року, зумовила необхідність посилення захисту даних в українських інформаційно-комунікаційних системах.

У зв'язку з цим 15 березня 2022 року Верховна Рада України прийняла за основу та в цілому Закон «Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів» за № 7152. 16 березня цей Закон був відправлений на підпис Президенту України.

У проекті Закону зазначається, що «власники системи для забезпечення належного функціонування систем та захисту інформації, що обробляється в них … можуть розміщувати державні інформаційні ресурси та їх резервні копії на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України, протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування».

Центри обробки даних можуть бути розташовані у будь-якій точці земної кулі. У зв'язку з цим у проекті Закону додатково зазначається: «Забороняється ведення публічних електронних реєстрів, за допомогою хмарних ресурсів та/або центрів обробки даних, що розміщені на території України, де органи державної влади України тимчасово не здійснюють свої повноваження, територіях держав, визнаних Верховною Радою України державами-агресорами, територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції», та територіях держав, які входять до митних та воєнних союзів з такими державами» [1].

У практичній діяльності актуальними є питання, пов'язані із забезпеченням безпеки зберігання даних у віддалених центрах обробки даних (англ. – Data Center, далі – «ЦОД»).

Поширеною є думка про те, що зберігання даних у спеціалізованих ЦОД є повністю безпечним. Однак це не так.

Так, 10 березня 2021 року пожежа знищила ЦОДи SBG2 та SBG1, що належали одному з найбільших хостинг-провайдерів у Європі, компанії OVH. Під час пожежі згоріло як обладнання, так і резервні копії даних SBG2, що зберігалися в сусідньому SBG1. Як засвідчило розслідування інциденту, причиною пожежі стала несправність системи безперебійного живлення [2]. Крім того, швидкому поширенню вогню сприяла невдало спроектована система вентиляції будівлі та відсутність систем

автоматичного пожежогасіння. До слова, відсутність автоматичних систем пожежогасіння пов'язана з тим, що їхня наявність у деяких країнах Євросоюзу не є обов'язковою вимогою для власників будівель.

У цьому разі причиною пожежі стала система, основним завданням якої було забезпечення безпеки зберігання даних. Наслідком пожежі стали збої в роботі та недоступність для користувачів приблизно 3,6 млн. веб-сайтів.

Пожежі в ЦОД трапляються достатньо регулярно. Так, за даними організації Uptime Institute, подібні події трапляються приблизно раз на рік, і не завжди ці пожежі вдасться вчасно локалізувати [3].

Крім того, відомі випадки, коли причиною непрацездатності ЦОД стали несприятливі погодні умови. Наприклад, 4 вересня 2018 року сильна гроза в Техасі призвела до аварійного відключення основних джерел електропостачання кількох ЦОД компанії Microsoft, а системи резервного електропостачання, що були в них, вийшли з ладу. На усунення наслідків пішло кілька днів, протягом яких спостерігалися перебої з роботою сервісів Microsoft у світі [4].

За оцінками компанії Gartner, приблизні збитки, викликані відключенням ЦОД внаслідок аварії, можуть становити до 5,6 тис. дол. за хвилину [5].

Таким чином, очевидно, що до питання вибору конкретного ЦОД для зберігання критично важливої інформації слід підходити дуже виважено.

Критерієм вибору може бути категорія, присвоєна конкретному ЦОД організацією Telecommunications Industry Association («Асоціація телекомунікаційної галузі», TIA). Ця асоціація, створена 1988 року, зараз об'єднує близько 400 компаній, завданням яких є обговорення та вироблення галузевих стандартів у сфері інформаційних та комунікаційних технологій. Асоціацією були розроблені такі, наприклад, стандарти, як TIA-942 (стандарт телекомунікаційної інфраструктури для ЦОД) та TIA-569-B (стандарти для будівель ЦОД) [6]. Якщо дата-центр не має сертифікатів Uptime Institute – це ЦОД із *заявленим* рівнем Tier, якщо сертифікати є – це *підтверджений* рівень.

Усього існує чотири рівні оцінки ЦОД, що позначаються як Tier 1…4. Нижнім рівнем вважається перший, найвищим – четвертий.

ЦОД проходять сертифікацію TIA у три незалежні етапи. На першому етапі (Tier Certification of Design) перевіряється проектна документація на будівництво будівель ЦОД та пов'язаних з ними систем комунікацій, доступність під'їздів до будівлі для пожежної та інших служб. На другому етапі (Construction Tier Certification) здійснюється нагляд за процесом будівництва. На третьому етапі проводиться перевірка працездатності систем та якість обслуговування (кваліфікація персоналу). Після успішного проходження всіх трьох етапів TIA надає ЦОД певний рівень.

Рівень Tier I – є базовим і включає мінімальний набір необхідного обладнання (комп'ютери, комунікаційне обладнання, джерела безперебійного живлення, система кондиціювання, резервний електрогенератор). Системи резервування основного устаткування на цьому рівні

відсутні, а припустимий річний простій не повинен перевищувати 29 годин на рік. Відмовостійкість на цьому рівні становить 99.671 %. Такий рівень підходить для серверних підприємств. Через відсутність систем резервування, будь-яка відмова призведе до загальної непрацездатності системи на якийсь час.

Рівень Tier II – включає все, що є на рівні Tier I, додатково вводиться резервування критично важливих компонентів, що підключаються після проблем з основними. Електроживлення здійснюється через єдине введення. Такий рівень підходить для серверних середніх підприємств, допустимий річний простій не повинен перевищувати 22 години на рік. Відмовостійкість на цьому рівні становить 99.749 %.

Рівень Tier III – включає все, що є на рівні Tier II, додатково вводиться резервне введення електроживлення (від іншої магістральної лінії електропостачання, не пов'язаної з першою), наявність дизель-генератора на випадок відключення обох магістральних ліній електроживлення, використовуються промислові, а не побутові системи кондиціювання, наявність систем протипожежної безпеки та установок газового пожежогасіння. Крім того, ЦОД повинен розміщуватися в окремій будівлі, що знаходиться на території, яка охороняється. Головною особливістю ЦОД рівня Tier III є можливість безперебійного продовження роботи під час технічного та планового обслуговування.

ЦОДи рівня Tier III зараз є основою підтримки хмарних структур великих підприємств, служать основним майданчиком для компаній, які надають послуги хостингу, і, по суті, є у суспільній свідомості символом самого поняття «ЦОД».

Допустимий річний простій не повинен перевищувати 1 години та 10 хвилин на рік. Відмовостійкість на цьому рівні становить 99.982 %.

Рівню Tier III відповідають тільки шість ЦОД в України.

Рівень Tier IV включає все, що є на рівні Tier III, додатково здійснюється дублювання всіх основних і додаткових інженерних систем ЦОД. При цьому основні та резервні компоненти системи повинні знаходитись у різних приміщеннях будівлі ЦОД. Допустимий річний простій не повинен перевищувати 26 хвилин на рік. Відмовостійкість на цьому рівні становить 99.995 %.

ЦОД рівня Tier IV в Україні поки що немає.

ЦОД також можуть отримати рівень сертифікації за бронзовим, срібним або золотим рейтингом. Бронзовий рейтинг означає, що критерії сертифікації були виконані, однак є значні можливості для вдосконалення будівель та обладнання ЦОД для використання всього потенціалу інфраструктури. Золота сертифікація свідчить про те, що організація функціонує на повний потенціал встановленої інфраструктури.

Враховуючи важливість своєчасного доступу до критично важливих державних даних, для забезпечення належного функціонування систем та захисту інформації, що обробляється в них, державні інформаційні ресурси та їх резервні копії в центрах обробки даних, що розташовані за межами України, повинні бути розміщені в ЦОД, що відповідають рівню Tier IV.

Список використаних джерел:

1. Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів: Проект Закону України № 7152 від 13.03.2022. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/39215. – Дата звернення: 05.06.2022 р.
2. Fire Has Destroyed OVH's Strasbourg Data Center (SBG2). – URL: https://www.datacenterknowledge.com/uptime/fire-has-destroyed-ovh-s-strasbourg-data-center-sbg2. – Last access: 27.05.2022.
3. Uptime Institute Issued Awards. – URL: https://uptimeinstitute.com/uptime-institute-awards/list. – Last access: 27.05.2022.
4. Postmortem: VSTS 4 September 2018. – URL: https://devblogs.microsoft.com/devopsservice/?p=17485. – Last access: 27.05.2022.
5. BusinessViews: список самых крупных аварий в дата-центрах мира. – URL: https://businessviews.com.ua/ru/business/id/avarii-v-data-centrah-2248. – Дата обращения: 27.05.2022 г.
6. Telecommunications Industry Association: Standards. – URL: https://www.datacenterknowledge.com/uptime/fire-has-destroyed-ovh-s-strasbourg-data-center-sbg2. – Last access: 05.06.2022.

Ключові слова: хмарні технології, державні інформаційні ресурси, відмовостійкість, стандарти телекомунікаційної інфраструктури.

Key words: cloud technologies, state information resources, fault tolerance, telecommunication infrastructure standards.

ЩЕРБИНА ЮРІЙ ВОЛОДИМИРОВИЧ

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

КАЗАКОВА НАДІЯ ФЕЛІКСІВНА

Національний університет «Одеська юридична академія»,
професор кафедри кібербезпеки, доктор технічних наук, професор

РАНДОМІЗАЦІЯ ПРОГРАМНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Сучасний розвиток обчислювальної техніки робить комп'ютерне моделювання важливим етапом проектування технічних систем, які забезпечують коректне протікання таких складних процесів як розподілення потоків в транспортних та інформаційно-телекомунікаційних системах, в управлінні виробництвом та інфраструктурними і подібними їм складними об'єктами.