ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від _____ 2024 р. № _____

ПОРЯДОК
підтвердження відповідності вимогам до надавачів хмарних послуг та/або послуг центру обробки даних та вимоги до таких надавачів

1. Ці Порядок та вимоги та визначають заходи, які повинні бути виконані надавачем хмарних послуг та/або послуг центрів обробки даних (далі – надавач) для внесення його до переліку надавачів хмарних послуг та/або послуг центру обробки даних (далі - перелік надавачів), та механізм підтвердження відповідності вимогам.

2. У цих Порядку та вимогах терміни вживаються у значенні, наведеному в Законах України “Про електронні комунікації”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про технічні регламенти та оцінку відповідності”, “Про критичну інфраструктуру”, “Про основні засади забезпечення кібербезпеки України”, “Про хмарні послуги”.

3. Надавач має відповідати вимогам, визначеним у статті 8 Закону України “Про хмарні послуги”, а також вжити технічних та організаційних заходів для управління ризиками, що виникають для безпеки електронної комунікаційної мережі, електронної комунікаційної послуги та інформаційних систем, які використовуються для надання хмарних послуг, зазначених у цих Порядку та вимогах.

4. Безпека системи та устаткування забезпечується впровадженням системи управління інформаційною безпекою (далі – СУІБ) та/або комплексної системи захисту інформації з підтвердженою відповідністю за результатами державної експертизи у сфері технічного захисту інформації.

5. СУІБ, має передбачати:

1) автоматичний контроль за розподілом обов’язків працівників надавача;

2) політику інформаційної безпеки, яка включає:
цілі безпеки та її рівень;
зобов’язання надавача щодо запровадження заходів захисту, необхідних для досягнення встановлених цілей безпеки;
шляхи досягнення поставлених цілей безпеки;

організаційну структуру, призначену для забезпечення безпеки інформації, періодичність перегляду політики безпеки інформації, що має здійснюватися не менше одного разу на рік;

обов'язки надавача, користувачів хмарних послуг (далі – користувач) та інших учасників, залучених до надання хмарних послуг, заходи, направлені на забезпечення безпеки, вимоги законодавства у сфері захисту інформації та кібербезпеки, що застосовуються;

3) документи, що визначають порядок обробки персональних даних, чи політики, якими регламентовано дотримання конфіденційності обробки персональних даних;

4) вимоги до кваліфікації персоналу;

5) визначення ризиків порушення конфіденційності, цілісності та доступності інформації в межах СУІБ, їх оцінка та аналіз наслідків таких порушень; план заходів щодо зменшення або уникнення ризиків внаслідок реалізованих заходів захисту;

6) заходи перевірки кваліфікації та забезпечення дотримання дисципліни працівниками, які отримують доступ до даних користувача або технічних засобів, на яких вони зберігаються;

7) визначення приміщень, будівель, споруд, які використовуються для надання хмарних послуг, встановлення обмежень до зон доступу та впровадження контролю доступу до таких зон.

Контроль доступу забезпечується:

визначенням умов доступу до зон для працівників в залежності від їх трудових обов'язків, відвідувачів, зокрема обмеженням часу перебування у цих зонах;

необхідністю використання, принаймні, двох факторів автентифікації у разі доступу до зон, де розміщуються компоненти системи, які обробляють дані користувачів;

впровадженням автоматичного контролю за реєстрацією доступу до зон, заходів щодо індивідуального відстеження відвідувачів під час їх роботи в приміщеннях та будівлях, заходів, які забезпечують своєчасне виявлення та запобігання несанкціонованому доступу;

8) впровадження системи захисту устаткування, що включає, зокрема захист: кабелів електроживлення та зв'язку від перехоплення, завад або пошкоджень, устаткування під час його обслуговування або транспортування.

Процедури щодо захисту устаткування забезпечуються:

регулярними перевірками захисту кабелів електроживлення та зв'язку; визначенням порядку передачі устаткування, на якому зберігаються дані користувача, для його утилізації за межами відповідної зони захисту; своєчасним встановленням на устаткуванні оновлень з безпеки;

шифруванням даних користувача або їх безповоротним знищенням на устаткуванні, яке містить носії з даними користувача, перед передачею третій особі;

шифруванням даних на змінних та резервних носіях, що переміщуються між зонами доступу;

9) запровадження захисту від шкідливого програмного забезпечення.

Захист від шкідливого програмного забезпечення забезпечується:

встановленням захисних програм на компонентах систем, що використовуються для надання хмарних послуг у виробничому середовищі;

встановленням захисних програм на кінцевому устаткуванні працівників;

проведенням перевірок устаткування на наявність шкідливого програмного забезпечення;

оновленням антивірусних програмних засобів з максимальною частотою, яку пропонують постачальники таких засобів;

10) запровадження резервного копіювання та відновлення даних.

Резервне копіювання та відновлення даних забезпечуються:

встановленням обсягу та частоти резервного копіювання даних, та тривалості зберігання даних, які повинні відповідати умовам договорів із користувачами, а також вимогам безперервності роботи;

зберіганням резервних копій у зашифрованому форматі;

обмеженням доступу до резервних копій та виконанням відновлення лише визначеними надавачем особами;

проведенням тестування процедур відновлення не рідше одного разу на рік;

11) впровадження заходів захисту від кібератак.

Захист від кібератак забезпечується:

технічними заходами захисту щодо виявлення кібератак та реагування на них;

впровадженням технічних заходів для блокування приєднання сторонніх пристроїв (фізичних або віртуальних) до мережі (фізичної чи віртуальної) надавача;

застосуванням різних засобів технічного захисту для запобігання можливості подолання усіх рівнів захисту у випадку подолання одного елементу захисту;

12) запровадження вимог з безпеки для з’єднань всередині власної мережі.

Зазначені вимоги повинні передбачати, зокрема:

відокремлення логічної та фізичної сегментації з’єднань, що використовують користувачі;

дозволені внутрішні з’єднання та з’єднання між різними місцями обробки даних;

визначення дозволених з’єднань між різними мережами.

6. Надавач забезпечує цілодобову охорону приміщень, будівель, споруд, які використовуються для надання хмарних послуг.

7. Врегулювання інцидентів забезпечується:

1) запровадженням технічних та організаційних заходів, для реагування на всі відомі загрози безпеки;

2) розробкою настанов щодо класифікації, встановлення пріоритетів та ескалації інцидентів безпеки;

3) створенням групи реагування на надзвичайні ситуації, для скоординованого врегулювання інцидентів безпеки;

4) інформуванням про інциденти безпеки користувачів, яких цей інцидент стосується;

5) збиранням даних про інциденти безпеки та аналізом типових інцидентів безпеки;

6) регулярним тестуванням заходів реагування на інциденти безпеки з метою встановлення їх ефективності та виявлення недоліків;

7) повідомленням Адміністрації Держспецзв’язку та CERT-UA про будь-який інцидент, який має значний негативний вплив на надання хмарної послуги, у порядку, затвердженому Адміністрацією Держспецзв’язку.

Якщо вказаний вплив поширюється на державні електронні інформаційні ресурси, інформацію, вимога щодо захисту якої встановлена законом, або критичну інформаційну інфраструктуру CERT-UA невідкладно інформує Ситуаційний центр забезпечення кібербезпеки Служби безпеки України.

8. Управління безперервністю функціонування забезпечується:

1) плануванням можливих сценаріїв, розроблених за результатами аналізу ризиків;

2) визначенням пріоритетних систем надавача, зупинка функціонування яких призведе до негативних наслідків надання та/або припинення надання хмарних послуг;

3) оцінкою залежності сталого надання хмарних послуг від ресурсів, програмного забезпечення, субпідрядників, постачальників послуг, товарів, робіт;

4) прогнозуванням наслідків запланованих і незапланованих перерв у наданні хмарних послуг, збоїв в роботі хмарних ресурсів, що можуть відбуватися впродовж певного часу;

5) визначенням максимально допустимого строку перерв у наданні хмарних послуг, та усунення збоїв в роботі хмарних ресурсів;

6) наявністю ресурсів, необхідних для відновлення роботи у визначені строки;

7) впровадженням плану забезпечення безперервної діяльності;

8) упорядкуванням процесів, пов’язаних з функціонуванням хмарних ресурсів, а саме щодо:

закупівлі, введення в експлуатацію, технічного обслуговування, виведення з експлуатації та утилізації хмарних ресурсів;

ведення обліку хмарних ресурсів та маркування технічних засобів в залежності від визначених рівня захисту та заходів захисту інформації;

підтримання безпечної конфігурації механізмів обробки помилок, реєстрації подій, шифрування, аутентифікації та авторизації;

визначення вимог та процедур щодо використання версій програмного забезпечення та його оновлення, правил поводження з програмним забезпеченням, підтримка якого більше не здійснюється;

запровадження обмежень на встановлення програмного забезпечення або використання хмарних послуг;

запровадження віддаленої деактивації, видалення або блокування;

повного та незворотного видалення (знищення) даних при виведенні хмарного ресурсу з експлуатації;

видів та порядку проведення оновлень, пов’язаних вимог до обсягу тестування, та отримання необхідних погоджень;

вимог до виконання тестування;

вимог до виконання термінових оновлень;

9) запровадженням технічних та організаційних заходів для моніторингу надання та припинення надання хмарних послуг, зокрема необхідних для забезпечення виконання умов договору про рівень обслуговування.

9. Надавач має запровадити інформування про поточні загрози та програми навчання працівників щодо безпеки інформації, які повинні охоплювати, зокрема питання:

поводження з системними компонентами, які використовуються для надання хмарних послуг у виробничому середовищі;

поводження з даними користувачів;

дій у разі виникнення інцидентів безпеки.

10. Надавач повинен розміщувати інформацію про наявність та доступність хмарних ресурсів, з якою користувач може ознайомитись з використанням мережі Інтернет, а також забезпечити користувачам можливість здійснення контролю за розподілом призначених їм системних ресурсів.

11. Надавач повинен запровадити заходи автоматизованого контролю за наданням хмарних послуг.

12. Моніторинг, аудит та випробування забезпечується:

1) запровадженням механізмів реєстрації та моніторингу подій на компонентах системи, які мають передбачати:

визначення подій, які можуть призвести до порушення інформаційної безпеки;

умови для початку, зупинки та призупинення реєстрації подій;

інформацію про призначення та терміни зберігання журналів реєстрації подій;

визначення працівників, що відповідають за реєстрацію подій та моніторинг ведення журналів реєстрації подій;

синхронізацію часу системних компонентів;

2) запровадженням планування та проведення аудитів щодо:

виявлення дій, які можуть призвести до перерв/збоїв у наданні послуги або порушень умов договорів, виконуються під час планового технічного обслуговування;

реєстрації та моніторингу усіх дій;

3) регулярним (не менш ніж один раз на місяць) проведенням випробувань (тестів) для виявлення загальновідомих вразливостей системних компонентів, які використовуються для надання послуг;

4) проведенням випробувань (тестів) на можливість обходу та/або деактивації засобів захисту відповідно до задокументованої методології, які мають проводитися персоналом надавача, що має відповідну кваліфікацію, або із залученням третіх осіб, які надають відповідні послуги;

5) аналізом результатів випробувань (тестів) на проникнення та усуненням виявлених вразливостей.

13. Надавач повинен проводити не рідше одного разу на рік внутрішні аудити для перевірки відповідності системи внутрішнього контролю безпеки, вимогам, визначеним цими Порядком та вимогами (далі – вимоги до надавача).

14. Надавач забезпечує відповідність міжнародному стандарту ISO/IEC 27001 або національному стандарту іноземної країни, прийнятому відповідно до міжнародного стандарту ISO/IEC 27001, або ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27018:2019 «Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII» (ISO/IEC 27018:2019, IDT).

15. Підтвердження відповідності вимогам до надавача, є обов’язковим для внесення відомостей про надавача до переліку надавачів, ведення якого здійснюється регулятором комунікаційних послуг.

16. Відповідність вимогам до надавача підтверджується:

1) документом про відповідність, виданим органом з оцінки відповідності, та/або документом з підтвердження відповідності, комплексної системи захисту інформації за результатами державної експертизи у сфері технічного захисту інформації;

2) документами, що визначають порядок обробки персональних даних чи політики, якими регламентовано дотримання конфіденційності обробки персональних даних;

3) документами, що підтверджують право власності або право користування засобами, що використовуються при наданні хмарних послуг та/або послуг центру обробки даних у разі відсутності такої інформації в публічних електронних реєстрах, інформаційно-комунікаційних системах;

4) документами, що підтверджують право власності або право користування приміщеннями, що використовуються для розміщення всіх складових програмно-технічного комплексу, що забезпечують надання хмарних послуг для надавачів послуг центру обробки даних;

5) документом про відповідність, виданим органом з оцінки відповідності у сфері електронних комунікацій, що підтверджує відповідність юридичних осіб, фізичних осіб – підприємців, які мають намір надавати хмарні послуги та/або послуги центру обробки даних, цим Порядку та вимогам.

17. Регулятор комунікаційних послуг після отримання заяви про внесення до переліку надавачів забезпечує перевірку достовірності, повноту поданих надавачем документів та відомостей.

18. Достовірність, зазначених у заяві реквізитів документів, передбачених підпунктами 2, 4, 5 пункту 16 цих Порядку та вимог, перевіряється регулятором комунікаційних послуг шляхом доступу до відповідних інформаційно-комунікаційних систем або в автоматичному режимі шляхом електронної інформаційної взаємодії відповідно до Порядку електронної (технічної та інформаційної) взаємодії, затвердженого постановою Кабінету Міністрів України від 08 вересня 2016 року № 606 (Офіційний вісник України, 2016 р., № 73, ст. 2455).

У разі відсутності технічної можливості передачі даних у спосіб, визначений абзацом першим цього пункту, електронна інформаційна взаємодія суб’єктів інформаційних відносин може здійснюватися з використанням інших інформаційно-комунікаційних систем із застосуванням в них відповідних комплексних систем захисту інформації з підтвердженою відповідністю за результатами державної експертизи в порядку, встановленому законодавством у сфері захисту інформації та кібербезпеки.

У випадку неможливості отримання відомостей шляхом електронної інформаційної взаємодії, регулятор комунікаційних послуг надсилає до суб’єкта, який видав документи (далі - суб’єкт), запит щодо підтвердження видачі такого документа та/або достовірності відомостей.

Суб’єкт протягом п’яти робочих днів з дня отримання запиту щодо підтвердження видачі відповідного документа та/або достовірності відомостей підтверджує або заперечує видачу відповідного документа та/або достовірність відомостей з використанням системи електронної взаємодії електронних ресурсів або відповідної інформаційно-комунікаційної системи.

Якщо протягом п’яти робочих днів з дня отримання суб'єктом запиту, відповідь на запит щодо підтвердження або заперечення видачі відповідного документа та/або достовірності відомостей від суб’єкта не отримано, вважається що надана надавачем інформація є достовірною.

_____