Додаток 1 до листа Телекомпалати України від 26.04.2024 р. № 2843

Порівняльна таблиця
пропозицій та зауважень операторів електронних комунікацій до розробленого Адміністрацією Держспецзв'язку проекту наказу «Про затвердження Порядку повідомлення про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг центру обробки даних»

Редакція запропонована Адміністрацією Держспецзв'язку	Пропозиції та зауваження операторів електронних комунікацій	Обгрунтування
Адміністрація Державної служби спеціального зв'язку та захисту інформації України		
НАКАЗ		
Про затвердження Порядку повідомлення про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг центру обробки даних		
Відповідно до абзацу четвертого частини першої статті 8 Закону України "Про хмарні послуги", підпункту 7^2 пункту 4 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411,		
НАКАЗУЮ:		
1. Затвердити Порядок повідомлення про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг центру обробки даних, що додається.		

2. Департаменту державного регулювання у сфері комунікаційних послуг Адміністрації Державної служби спеціального зв'язку та захисту інформації України забезпечити подання цього наказу в установленому порядку на державну реєстрацію до Міністерства юстиції України.		
3. Цей наказ набирає чинності з дня його офіційного опублікування.		

Порівняльна таблиця
пропозицій та зауважень операторів електронних комунікацій до розробленого Адміністрацією Держспецзв'язку проекту Порядку повідомлення про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг центру обробки даних

Редакція запропонована Адміністрацією Держспецзв'язку	Пропозиції та зауваження операторів електронних комунікацій	Обгрунтування
Порядок повідомлення про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг центру обробки даних		
1. Цей Порядок визначає вимоги щодо моніторингу надавачами хмарних послуг та/або послуг центру обробки даних (далі – надавачі послуг) інцидентів, які мають значний негативний вплив на надання хмарної послуги та/або послуг центру обробки даних, оповіщення про такі інциденти та реагування на них.	1. Цей Порядок визначає вимоги щодо **інформування надавачами хмарних послуг та/або послуг центру обробки даних (далі – надавачі послуг) про інциденти, які мають значний негативний вплив на надання хмарної послуги та/або послуг центру обробки даних.**	Запропонована розробником редакція не відповідає назві документу та положенням абзацу четвертого частини першої статті 8 Закону України "Про хмарні послуги".
2. У цьому Порядку терміни вживаються у такому значенні:		
інцидент – незапланована подія, що призвела до часткового або повного		

виходу з ладу або зниження ефективності функціонування послуги;		
Відсутній	**Інцидент зі значним негативним впливом – інцидент, який суттєво загрожує сталому, надійному та штатному режиму функціонування електронної комунікаційної мережі, електронної комунікаційної послуги та інформаційних систем, які використовуються для надання хмарних послуг, внаслідок чого виникає значний негативний вплив на надання хмарної послуги та/або послуг ЦОД або призводить до неможливості надання таких послуг.**	Доповнення визначенням основного терміну, відносно якого розроблено проект документу.
негативний вплив – вплив інциденту на процес надання хмарної послуги, який призводить до зміни функціональних можливостей послуги або робить її недоступною.		
3. Інші терміни, що використовуються у цьому Порядку, вживаються у значенні, наведеному в Законах України «Про хмарні послуги» і «Про основні засади забезпечення кібербезпеки України».		
4. Надавачі послуг вживають відповідних пропорційних технічних	**Виключити**	Зміст не відповідає назві та меті документу, що визначені Законом.

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 та/або послуг центру обробки даних (далі – ЦОД), заходів з реагування на інциденти.		
Реагування на будь-який інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг ЦОД, здійснюється надавачами послуг шляхом вжиття заходів, спрямованих на швидке виявлення та захист від таких інцидентів, належне інформування про них регулятора комунікаційних послуг та урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, запобігання негативним наслідкам, їх мінімізації та усунення, виправлення вразливостей, а також відновлення сталості і надійності функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем та інших об'єктів, що використовуються для		

надання хмарної послуги та/або послуг ЦОД.		
5. Заходи з реагування на інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг ЦОД, проводяться надавачами послуг послідовно за такими етапами: підготовка; виявлення загроз та аналіз наслідків інциденту для подальшого надання відповідної хмарної послуги; усунення загроз безпеці та відновлення можливості надавати послуги; аналіз ефективності заходів з реагування на інцидент; звіт.	**Виключити**	Зміст не відповідає назві та меті документу, що визначені Законом.
6. Реагування надавачами послуг розпочинається з етапу підготовки, під час якого проводяться заходи з вивчення та дослідження можливих інцидентів при наданні/отриманні відповідних видів хмарних послуг та/або послуг ЦОД, що є критичними для надавачів і користувачів цих послуг, розроблення методів і механізмів запобігання та протидії можливим інцидентам.	**Виключити**	Зміст не відповідає назві та меті документу, що визначені Законом.
7. На етапі виявлення загроз та аналізу наслідків інциденту для подальшого	**Виключити**	Зміст не відповідає назві та меті документу, що визначені Законом.

надання відповідної хмарної послуги надавачі послуг здійснюють виявлення інциденту та визначають його критичність для забезпечення пропорційності та/або відповідності подальших заходів реальним і потенційним ризикам.		
Надавачі послуг визначають критичність інциденту за такими пріоритетами:	**Виключити**	Зміст не відповідає назві та меті документу, що визначені Законом.
низький пріоритет – інцидент має незначний вплив на сталий, надійний і штатний режим функціонування електронної комунікаційної мережі, електронної комунікаційної послуги та інформаційних систем, які використовуються для надання хмарних послуг та/або послуг ЦОД, або взагалі не несе загроз та усувається надавачем послуг автоматично або з втручанням адміністратора системи моніторингу інцидентів протягом одного робочого дня;	**Виключити**	Зміст не відповідає назві та меті документу, що визначені Законом.
середній пріоритет – інцидент безпосередньо впливає на сталий, надійний та штатний режим функціонування електронної комунікаційної мережі, електронної комунікаційної послуги та	**Виключити**	Зміст не відповідає назві та меті документу, що визначені Законом.

інформаційних систем, які використовуються для надання хмарних послуг та/або послуг ЦОД, але загроза несе незначний негативний вплив на надання цих послуг і своєчасно усувається надавачем послуг протягом 4 годин;		
високий пріоритет – інцидент безпосередньо загрожує сталому, надійному та штатному режиму функціонування електронної комунікаційної мережі, електронної комунікаційної послуги та інформаційних систем, які використовуються для надання хмарних послуг, внаслідок чого виникає негативний вплив на процес надання хмарної послуги та/або послуг ЦОД, але не робить її недоступною. Інцидент обробляється максимально швидко надавачем послуг та загроза усувається протягом 2 годин;	**Виключити**	Зміст не відповідає назві та меті документу, що визначені Законом.
найвищий пріоритет – інцидент суттєво загрожує сталому, надійному та штатному режиму функціонування електронної комунікаційної мережі, електронної комунікаційної послуги та інформаційних систем, які використовуються для надання хмарних послуг, внаслідок чого	**Виключити**	Зміст не відповідає назві та меті документу, що визначені Законом.

виникає значний негативний вплив на надання хмарної послуги та/або послуг ЦОД або призводить до неможливості надання таких послуг. Зазначений інцидент потребує невідкладного реагування надавача послуг, максимального залучення сил і засобів урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA і суб'єктів забезпечення кібербезпеки.		
Відсутній	**Інцидент зі значним негативним впливом потребує невідкладного реагування надавача послуг, максимального залучення сил і засобів урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA і суб'єктів забезпечення кібербезпеки.**	Визначення першочергових заходів при виявленні інциденту зі значним негативним впливом.
Про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг ЦОД, надавач послуг невідкладно інформує регулятора комунікаційних послуг та урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA.		
Повідомлення про такий інцидент має бути подано надавачем послуг		

протягом години з моменту його виявлення шляхом надсилання електронних листів із застосуванням положень Законів України «Про електронні документи та електронний документообіг» та «Про електронні довірчі послуги» за формою, наведеною у додатку до цього Порядку.		
У разі відсутності технічної можливості надіслати електронний лист дозволяється надсилати належним чином завірену копію зазначеного повідомлення.	**Виключити**, або внести уточнення щодо технічної реалізації цієї вимоги.	Незрозуміло яким чином (якими способами та засобами) направляти документ для забезпечення повідомлення протягом години. Також зайвою є вимога щодо «завіреної копії» - повідомлення підписується уповноваженою особою.
8. Метою етапу усунення загроз безпеці та відновлення можливості надавати послуги є відновлення штатного режиму функціонування шляхом ліквідації наслідків інциденту. Заходи з ліквідації наслідків та відновлення можливості надавати послуги можуть бути виконані одночасно.	**Виключити**	Зміст не відповідає назві та меті документу, що визначені Законом.
9. За результатами вжитих заходів надавачі послуг проводять аналіз ефективності реагування на інциденти,	**Виключити**	Зміст не відповідає назві та меті документу, що визначені Законом.

а також забезпечують узагальнення та проведення аналізу досвіду реагування для подальшого підвищення ефективності вжиття відповідних заходів у разі можливих інцидентів у майбутньому.		

Пропозиції та зауваження просимо вносити безпосередньо до тексту Форми заяви та виділяти кольором

Додаток
до Порядку повідомлення про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг центру обробки даних
(пункт 7)

Повідомлення
про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг ЦОД

1. _____

_____

(повне найменування надавача хмарних послуг та/або послуг ЦОД, місцезнаходження, адреса офіційної сторінки в мережі Інтернет (за наявності)

2. _____

_____

(посада, прізвище та власне ім'я посадової особи, яка повідомляє про інцидент, та її контактні дані (телефон, факс, e-mail)

3. _____

(час (у форматі година/хвилина/секунда) і дата виявлення інциденту)

4. _____

_____

(опис інциденту (спосіб, методи та засоби виявлення інциденту, джерело загрози, вплив на послугу, будь-яка інша важлива інформація)

5. _____

_____

(опис вкладень і додатків до повідомлення)

6. _____

_____

(посада, прізвище та власне ім'я посадової особи, відповідальної за усунення інциденту, та її контактні дані (телефон, факс, e-mail)

7. _____

(інформація про заходи реагування на інцидент)

ВИКЛЮЧИТИ п. 7 – протягом години має бути направлене повідомлення про виявлений інцидент. Заходи реагування та визначення їх результатів можуть займати більше часу в залежності від суті інциденту.

Засвідчую достовірність і повноту зазначених у цьому повідомленні відомостей та інформації.

«____» _____ 20 ___ року _____

(підпис керівника або особи,
яка може вчиняти дії від імені суб'єкта
господарювання,

або особисто фізичної особи - підприємця)

_____