denovo
Inspired by the future

# Справжня Приватна Хмара для державного сектору

# Зміст

# Як перестати боятися і полюбити хмару

> **Хмари для держсектора - тема особлива. Вони повинні бути екстремально надійними, продуктивними, функціональними, і до того ж для них необхідно отримати всі встановлені законом документи і сертифікати. Зокрема, без КСЗІ та ОТР тут не обійтися, що цілком логічно, враховуючи загрози безпеки і ціну потенційної помилки.**

Глобальна парадигма розвитку IT активно зміщується в бік хмарної моделі, а в 2019 році вперше за весь час витрати на хмари випередили витрати на залізо*. Оператори різних IaaS і SaaS-сервісів міцно увійшли в число найбільших світових компаній і це, схоже, тільки початок. Хмарний сегмент розвивається дуже швидко, а його обсяг обчислюється сотнями мільярдів $. Навіть в нашій країні, де IT-ринок відчуває регулярні стреси, хмари стабільно ростуть. Про технологічні і фінансові переваги подібного підходу говорилося чимало і комерційний сектор, в основній своїй масі, вже давно не сумнівається в необхідності роботи з хмарами.

Інша справа держструктури, де ступінь ризику і відповідальності вище. Навіть в найпрогресивніших і економічно розвинених країнах офіційні організації довгий час недовірливо придивлялися до хмарних сервісів, але в підсумку, зваживши ризики і усвідомивши вигоди, перейшли до використання на початку приватних платформ, а потім і захищених комерційних сервісів. Як наслідок, сьогодні в США, КНР, Великобританії, країнах ЄС державні структури входять до числа найбільших замовників хмарних послуг. Звичайно, не кожному оператору дозволять тримати у себе частину державних IT-інфраструктур і важливих даних - на вироблення критеріїв відбору майданчиків пішли роки і в кожній країні вони мають свої особливості.

У цьому плані Україна майже нічим не відрізняється від європейських і американських партнерів. Ми, з відставанням в кілька років, проходимо той же шлях від сумнівів до (будемо сподіватися) повного прийняттю концепції. Адже, коли мова йде про явища державної ваги, природно, не можна вірити на слово. Надійність і захищеність хмарної інфраструктури повинна бути підтверджена відповідністю національним стандартам і нормативам в області безпеки. Найбільш відомим документом в цьому плані можна назвати сертифікат відповідності КСЗІ. Ще одним ступенем підтвердження надійності хмари є наявність експертного висновку на організаційно-технічне рішення (ОТР). Отримати його в нашій країні дуже непросто, але, без

1) Згідно досліджень Synergy Research Group в 2019 році глобальні витрати на керовані приватні хмари виявились більшими на 1%, аніж витрати на ІКТ системи для ДЦ.

## Справжня приватна хмара для державного сектору

цього документа говорити про те, що хмара готова до прийому державних замовників, по суті, передчасно. Чому? Давайте розберемося.

> **27 серпня 2020 року De Novo, було видано експертний висновок на ОТР, зареєстроване в Адміністрації Державної служби спеціального зв'язку та захисту інформації під №1150,тому наша компанія не з чуток знає всі деталі цього процесу.**

## ОТР для інформації з обмеженим доступом

Офіційна, канцелярська, мова має чимало специфічних особливостей і зрозуміти, що ховається за певними формулюваннями, відразу буває дуже непросто. В даному випадку, “організаційно-технічне рішення” - це ні що інше як проект (“креслення”) апаратно-програмної платформи для розгортання хмарних сервісів.

Щоб оцінити її захищеність і надійність, уповноваженими органами проводиться спеціальна комплексна експертиза на відповідність вимогам цілого спектра нормативних документів, в числі яких Закони України “Про наукову і науково-технічну експертизу”, “Про захист інформації в інформаційно-телекомунікаційних системах”, “Про інформацію”; постанову Кабінету Міністрів України від 29 березня 2006 року № 373 “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах”; положення про державну експертизу в сфері технічного захисту інформації та інші акти нормативно-технічного характеру.

За результатами тривалого і докладного аналізу, а також всебічної перевірки, видається експертний висновок про відповідність ОТР зазначеним вимогам і про можливість використання рішення для обробки даних, необхідність технічного захисту яких визначена законодавством України. Зазвичай такою інформацією володіють державні структури, але, строго кажучи, експертний висновок ОТР КСЗІ не прив'язаний до типу організації і в рівній мірі є актуальним для всіх установ і компаній, незалежно від форми власності. У будь-якому випадку, наявність надійних механізмів технічного захисту інформації (ТЗІ), документально підтверджене національним регулятором, є важливим елементом побудови IT-інфраструктур, яка оброблює державні або бізнес-дані.

**Компанія De Novo першою в Україні отримала експертний висновок ОТР КСЗІ на власне комплексне хмарне рішення Hosted Private Infrastructure (приватне хмара за моделлю "як сервіс"). В ході оцінки здатності HPI забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядалися вимоги двох типів: до функцій захисту (сервісів безпеки) і, окремо, до гарантій.**

ЕКСПЕРТНИЙ ВИСНОВОК

Організаційно-технічне рішення на розгортання комплексної системи захисту інформації типової приватної хмарної інфраструктури

Зареєстровано в Адміністрації Державної служби спеціального зв'язку та захисту інформації України
"27" серпня 2020 р. за № 1150
Дійсний до "27" серпня 2025 р.

За результатами експертизи встановлено, що організаційно-технічне рішення для комплексної системи захисту інформації **типової приватної хмарної інфраструктури,**
(назва ОТР)

що належить **ТОВ «ДЕ НОВО»**
найменування організації (підприємства,

**м. Київ, вул. Північно-Сирецька, 1-3**
установи) – власника (розпорядника), місцезнаходження)

**відповідає**
(відповідає/не відповідає)

вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Технічне завдання на побудову організаційно-технічного рішення на розгортання комплексної системи захисту інформації типової приватної хмарної інфраструктури. UA.35877574.КСЗІ.00002.ТЗ».

Вимоги до сфери використання організаційно-технічного рішення та методів впровадження КСЗІ в ІТС на реальному об'єкті експлуатації наведені у відповідному розділі Експертного висновку.

**Директор ТОВ «ЗАХИСТ.ЮЕЙ»** **Н. І. Касьян**
підпис ініціали, прізвище

«ЗАХИСТЮЕЙ»

Кожна послуга являє собою набір інструментів, що дозволяють протистояти певному переліку погроз, і може містити кілька рівнів. Чим вище рівень послуги, тим повніше забезпечується захист від певного виду загроз. Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до сервісів, що забезпечує захист від загроз одного з чотирьох основних типів:

- **Конфіденційність.** Сюди входять загрози, пов'язані з можливістю несанкціонованого ознайомлення з інформацією, що має обмежений доступ. Рішення, яке відповідає вимогам ОТР має чітко розмежовувати доступ до тих або інших даних, реалізуючи повністю захищені політики інформаційної безпеки.
- **Цілісність.** Тут об'єднані загрози, що відносяться до несанкціонованої модифікації даних.
- **Доступність.** Якщо що-небудь призводить до порушення можливості використання самої платформи HPI або інформації, яка на ній обробляється, то цей фактор по визначенню є загрозою доступності. Протистояти їм можна, використовуючи різні механізми відмовостійкості і відновлення після збоїв.
- **Спостережність.** У цьому пункті визначаються засоби ідентифікації і контролю над діями користувачів, а також фактори керованості хмарної платформи. Тут визначені такі дії і поняття як: реєстрація, ідентифікація і аутентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, тощо.

Крім функціональних факторів, що дозволяють оцінити якість послуг безпеки для HPI, в документах експертизи описані також критерії гарантій, що визначають коректність реалізації послуг (вимоги до архітектури комплексу засобів захисту, середовища розробки, експлуатаційної документації та безлічі інших аспектів).

## Справжня приватна хмара для державного сектору

Завантажити повну версію