

УДК 346.34 + 347.73

DOI <https://doi.org/10.32837/apdp.v0i91.3252>

Ю. В. Хорт

РЕГУЛЮВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ У ФІНАНСОВОМУ СЕКТОРІ УКРАЇНИ

1. Вступ

Натепер у всьому світі (як у розвинених економіках, так і тих, що розвиваються) відбувається стрімка еволюція використання хмарних технологій як органами державної влади, так і комерційними організаціями й особливо організаціями фінансового сектору.

Згідно з даними McKinsey & Company використання хмарних технологій у банківському секторі вже становить 25% основної діяльності банків, і 40–90% банківського навантаження глобально могло б бути в публічній хмарі протягом 10 років. Finextra виявила, що фінансові установи Сінгапуру (42%) вже здійснюють платежі й іншу діяльність за допомогою хмарних технологій, слідуючи за США (33%) і Великобританією (30%) [1, с. 11].

Під час COVID-19-пандемії використання хмарних технологій тільки продовжує зростати, адже актуальність цифрових технологій важлива як ніколи; фінансові установи мають адаптуватися до нових умов – коли більшість їх роботи здійснюється дистанційно, водночас питання безпеки й гнучкості систем постають із новою силою [2].

Більшість розвинених юрисдикцій передбачають механізми розвитку використання хмарних технологій та активно створюють та удосконалюють законодавчу основу для їх регулювання.

Україна проголосила амбітну мету – створення Києва міжнародним фінансовим центром – і передбачає одним зі шляхів її досягнення розвиток використання хмарних технологій. Однак законодавча основа для їх розвитку й використання натепер відсутня, тому доцільно проаналізувати світовий досвід щодо законодавчого регулювання використання хмарних технологій.

Мета статті – дослідження переваг і ризиків щодо використання хмарних технологій у фінансовому секторі; аналіз стану й підходів до їх регулювання як в Україні, так і за кордоном; виявлення особливостей і проблем в їх регулюванні й надання відповідних рекомендацій щодо побудови моделі законодавчого регулювання хмарних технологій у фінансовому секторі України.

Огляд теоретичної літератури. В українській науковій літературі питання використання хмарних технологій досліджувалися в контексті проблем забезпечення інформаційної безпеки під час використання хмарних технологій органами державної влади; Сопільник та інші (2020 р.) звертають увагу на необхідність визначення критеріїв надійності й стійкості використовуваних інформаційно-комунікаційних технологій (далі – ІКТ), важливості сертифікації продуктів і послуг у сфері ІКТ [34]. Однак проблеми правового регулювання хмарних технологій

у фінансовому секторі України не отримали належного висвітлення. У зарубіжній юридичній літературі ці питання досліджені в низці праць, що містять аналіз економічної доцільності використання хмарних технологій (Capgemini Group (2011 р.) [3], Ян (2017 р.) [4]); проблем законодавчого регулювання хмарних технологій у страховому секторі (Крісанто й інші (2018 р.) [5]); впливу використання хмарних технологій фінансовими установами на фінансову стабільність (Рада фінансової стабільності (2019 р.)); дослідження проблем нагляду під час використання хмарних технологій фінансовими установами з позиції здійснення нагляду (Торонто центр (2020 р.) [7]). У порівнянні з попередніми роботами це дослідження містить:

1) огляд переваг і ризиків використання хмарних технологій (як у розвинених країнах, так і в тих, що розвиваються);

2) аналіз розвитку законодавчої основи щодо використання хмарних технологій в Україні;

3) ширшу сферу розгляду зарубіжного законодавства (як загального регулювання хмарних послуг, так і спеціального, що стосується безпосередньо фінансового сектору), враховуючи останні реформи станом на 2021 р., а також відмінностей у регулюванні ЄС щодо різних секторів фінансового ринку;

4) пропозиції щодо побудови моделі законодавчого регулювання хмарних технологій в Україні.

2. Переваги й ризики використання хмарних технологій

Питання переваг і ризиків використання хмарних технологій досліджувалися в багатьох наукових працях. Більшість досліджень виділяють такі переваги використання хмарних технологій у фінансовому секторі: скорочення витрат на ІТ; підвищення гнучкості й операційної ефективності роботи фінансових установ; можливість розробки інноваційних фінансових продуктів і послуг (Capgemini Group (2011 р.) [3, с. 4], Ян (2017 р.) [4, с. 30], Торонто Центр (2020 р.) [7, с. 4], Швейцарська фінансова рада [1, с. 13–14] та інші). Окремі дослідження виділяють також такі переваги використання хмарних технологій, як покращення протидії ризикам, включаючи посилення безпеки бізнесу й забезпечення інклюзивності й гендерної рівності (Торонто центр (2020 р.) [7, с. 4]), а також позитивний вплив використання хмарних технологій на клімат (Capgemini Group (2011 р.) [3, с. 4]).

Розглянемо детальніше ці **переваги використання хмарних технологій**:

1) їх використання сприяє *скороченню витрат на ІТ*, адже встановлення та обслуговування фізичного технічного обладнання може бути більш витратним; натомість під час використання хмарних технологій зменшується вартість зберігання та обробки даних, оскільки фінансові установи можуть використовувати хмарні технології за схемою «плати за використане» [3, с. 4; 1, с. 13];

2) *використання* хмарних технологій сприяє підвищенню гнучкості й операційної ефективності фінансових установ, що дозволяє збільшити швидкість уже впроваджених у них ІТ та операційних процесів завдяки їх більшій автоматизації та введенню інструментів самообслуговування [9, с. 7];

3) хмарні технології забезпечують *розробку інноваційних фінансових продуктів і послуг* шляхом забезпечення обчислювальної здатності для експериментів і розробок, скорочення термінів їх виконання, надання доступу до найновіших

технологій (таких як штучний інтелект і машинне навчання, включаючи аналітику великих даних), доступу до оновлень (таких як миттєві виправлення безпеки) і функцій [1; 7; 9];

4) використання хмарних технологій забезпечує *ефективну протидію ризикам*, адже вони посилюють ризик-менеджмент і підвищують стійкість для забезпечення безперервності обслуговування шляхом удосконалення управління даними й ризиками кібербезпеки [9, с. 7]. Зокрема, великі надавачі хмарних послуг (далі – НХП) можуть зменшити ці ризики шляхом спрямування ресурсів і значних інвестицій у захист даних і кібербезпеку, які досить часто недоступні окремим фінансовим установам;

5) хмарні технології забезпечують *інклюзивність і гендерну рівність*, а саме більший доступ, зокрема для осіб, які раніше мали невеликий доступ до фінансових продуктів, а також вони стимулюють інституційну різноманітність і конкуренцію, знижуючи вступні бар'єри [7, с. 4];

6) хмарні технології забезпечують позитивний вплив на клімат шляхом зменшення споживання енергії та викидів вуглецю в порівнянні з тими, що відбуваються під час створення фізичної ІТ інфраструктури [3, с. 4].

Однак зростають і певні **ризики від використання хмарних технологій**. Насамперед Крісанто й інші (2018 р.), Швейцарська фінансова рада (2020 р.) і Міжнародна організація комісій із цінних паперів (далі – IOSCO) (2020 р.) до них відносять:

1) *ризики безпеки* (кібер інциденти й витік даних);

2) *ризик втрати управління (контролю)* над функцією, переданою в аутсорсинг НХП, унаслідок відсутності повного розуміння фінансової установи, як ця функція буде виконуватися НХП;

3) *ризик оперативних збоїв у роботі НХП*;

4) *концентраційний ризик*, ураховуючи незначну кількість глобальних хмарних провайдерів, які займають вагому частину глобального ринку й тим створюють системний ризик;

5) *ризик країни (country risk)*, зокрема пов'язаний із географічним розташуванням НХП за кордоном [5, с. 11; 1, с. 12; 33, с. 9].

Додатково Крісанто й інші (2018 р.), Швейцарська фінансова рада (2020 р.) зазначають:

6) регуляторний або правовий ризик [1, с. 12; 5, с. 11].

А Крісанто й інші (2018 р.) і IOSCO (2020 р.) виділяють:

7) *проблеми нагляду за НХП* у випадку, якщо хмарні послуги мають транскордонний характер [5, с. 2; 33, с. 9].

Аналізуючи хмарні технології у фінансовому секторі, слід зазначити, що країни, що розвиваються, також активно їх впроваджують, однак у цих країнах переваги й ризики впровадження хмарних технологій у фінансовому секторі мають свої особливості. Насамперед хмарна інфраструктура може забезпечити більш стрімке зростання країнам, що розвиваються, у порівнянні з розвиненими економіками [8]:

1) спостерігається підвищена операційна ефективність і продуктивність фінансових установ, що використовують хмарні послуги;

2) значно простіше у фінансових установах, що використовують хмарні технології, впроваджувати інноваційні продукти й послуги, адже ці країни необтяжені застарілими системами й процесами, а тому може бути простіше їх впроваджувати;

3) хмарні технології можуть забезпечити надійний рівень безпеки, доступний для всіх фінансових установ [8];

4) хмарні технології надають необмежені можливості щодо зберігання даних і розвитку BigTech, насамперед для малих і середніх компаній [8].

Слід зауважити, що ризики під час використання хмарних технологій у фінансовому секторі в країнах, що розвиваються, теж мають свою специфіку:

1) ризики щодо захисту прав споживачів під час використання хмарних технологій у фінансовому секторі можуть бути більшими в цих країнах (наприклад, ширше використання даних компаніями BigTech через низьку фінансову грамотність клієнтів [10, с. 17];

2) в органів нагляду в країнах, що розвиваються, може бути обмаль ресурсів або спроможностей контролювати діяльність НХП [10, с. 22].

Отже, вигоди від використання хмарних технологій у фінансовому секторі очевидні й значно більші в порівнянні з ризиками від їх використання як у розвинених країнах, так і в країнах, що розвиваються. Тому зарубіжне законодавство йде шляхом дозволу використання хмарних технологій у фінансовому секторі, однак воно будується таким чином, щоб максимально протидіяти ризикам, що виникають.

3. Розвиток законодавчого регулювання хмарних послуг в Україні

Натепер в Україні відсутній комплексний підхід до регулювання хмарних послуг. Необхідність розвитку, стимулювання та, відповідно, законодавчого врегулювання хмарних технологій у фінансовому секторі України передбачено в низці програм і стратегій – Стратегії розвитку фінтеху в Україні до 2025 р. [11, п. 3.5.4, с. 35], Стратегії розвитку фінансового сектору України до 2025 р. [12, п. 5.4.4, с. 91] і в Національній економічній стратегії на період до 2030 р., затвердженої Кабінетом Міністрів України від 3 березня 2021 р. №179 [13].

Найбільш ґрунтовне бачення майбутнього розвитку хмарних послуг визначається в Національній економічній стратегії на період до 2030 р. Насамперед у ній зазначається, що «відсутність ефективної системи регулювання хмарних сервісів зменшує потенціал України на одному з найдинамічніших цифрових ринків». Також у Національній економічній стратегії на період до 2030 р. передбачається, що розвиток хмарних послуг має відбуватися шляхом:

1) закріплення принципу «насамперед хмарні технології» (Cloud First);

2) забезпечення сприятливих умов для побудови великих центрів обробки даних для хмарних сервісів;

3) надання підтримки експорту послуг хмарних обчислень і хмарних сховищ;

4) впровадження програми залучення для побудови інфраструктури хмарних сервісів міжнародних інвесторів і високотехнологічних компаній (Microsoft, Amazon, Alphabet, Alibaba, Facebook, Apple).

Також у Стратегії зазначається необхідність нормативного забезпечення можливості використання хмарних послуг. Ставиться за мету підвищення рівня використання хмарних технологій і віртуалізації для 90 відсотків бізнесу [13].

Слід зазначити, що спроби врегулювати хмарні послуги в Україні вже здійснювалися на рівні загального законодавства – у Проекті Закону України «Про хмарні послуги» № 2655 від 20 грудня 2019 р. У пояснювальній записці до цього законопроекту зазначається, що його метою є «створення умов для обробки й захисту даних під час використання технології хмарних обчислень, надання хмарних послуг і визначенні особливостей використання хмарних послуг органами державної влади, а також ефективнішого використання державних ресурсів шляхом впровадження новітніх технологій». До ключових положень пропонуваного регулювання в законопроекті належать:

1) визначення основних понять, таких як «хмарні обчислення», «хмарні послуги», «надавач хмарних послуг», «користувач хмарних послуг», «центр обробки даних»;

2) визначення та перелік хмарних послуг, способів їх надання, встановлення вимог до НХП для публічних замовників;

3) визначення істотних умов договору про надання хмарних послуг;

4) визначення особливостей надання та споживання хмарних послуг органами державної влади, органами місцевого самоврядування, державними організаціями, суб'єктами владних повноважень та іншими суб'єктами, яким делеговані такі повноваження, і захисту інформації під час надання хмарних послуг [14].

Оцінюючи зазначений законопроект (у тому числі в редакції до другого читання), слід зауважити, що такі важливі питання щодо використання хмарних послуг, як стандарти діяльності НХП, не регламентовані належним чином (зазначається, що НХП мають відповідати міжнародним стандартам, проте яким саме, не визначено); істотні умови договору про надання хмарних послуг також підлягають доповненню (зокрема порядок передачі НХП функцій, переданих йому на субаутсорсинг іншому НХП); порядок здійснення нагляду за НХП і обміну інформацією між різними органами, що здійснюють нагляд за НХП, доцільно регламентувати; законопроектом визначено, що регулювання та нагляд за діяльністю використання хмарних технологій банками, особами, що провадять діяльність на ринках фінансових послуг, здійснюється Національним Банком України. Вважаю, що регулювання та нагляд за діяльністю використання хмарних технологій фінансовими установами й іншими особами, що провадять діяльність на ринку капіталу, має здійснюватися Національною комісією із цінних паперів і фондового ринку.

Також у Стратегії розвитку фінтеху в Україні до 2025 р. і Стратегії розвитку фінансового сектору України до 2025 р. заплановано прийняття спеціального законодавства щодо хмарних послуг у фінансовому секторі.

Отже, український законодавець визнає важливість розвитку хмарних послуг в Україні, задекларувавши таку мету в низці програм і стратегій; здійснені спроби щодо створення загальної законодавчої основи щодо хмарних послуг, включаючи особливості користування ними органами державної влади, органами місцевого самоврядування та іншими суб'єктами, і аргументується необхідність регулювання хмарних послуг у фінансовому секторі. Однак перспективне законодавство у сфері хмарних послуг містить низку недоліків і підлягає удосконаленню.

4. Законодавча основа ЄС та інших зарубіжних країн щодо регулювання хмарних послуг у фінансовому секторі

Питанням регулювання використання хмарних послуг в ЄС приділяється значна увага вже протягом тривалого часу. Ще у 2012 році була розроблена Європейська хмарна стратегія, яка вперше визначила пріоритетом на рівні ЄС необхідність сприяння швидшому впровадженню хмарних обчислень у всіх секторах економіки [15]. Слід зазначити, що питання використання хмарних технологій в ЄС регламентовані як на рівні визначення загальних засад щодо регламентації діяльності НХП, так і на рівні спеціального законодавства, що стосується безпосередньо використання хмарних технологій у фінансовому секторі.

В ЄС відбувається розвиток загальних засад регламентації надання хмарних послуг передусім у напрямі надання НХП хмарних послуг належної якості й забезпечення безпеки використання хмарних технологій, що здійснюється шляхом:

1) розробки стандартів діяльності НХП. Так, 20 травня 2021 р. було прийнято добровільний до застосування Європейський хмарний кодекс поведінки [16], який було розроблено з метою забезпечення відповідності захисту даних у хмарному середовищі нормам ЄС, а саме Загальному регламенту ЄС про захист даних (далі – GDPR);

2) забезпечення сертифікації НХП, рекомендації щодо яких розроблені Робочою групою із сертифікації європейських НХП (2019 р.) [17]. Наступним кроком має бути розробка Агентством ЄС із питань мережевої та інформаційної безпеки (далі – ENISA) сертифікаційної схеми кібербезпеки для хмарних інфраструктур і послуг [18];

3) підвищення інформаційної обізнаності бізнесу про технічні й правові аспекти хмарних послуг. Із цією метою ЄС опублікувала Керівництво про Стандартизовані угоди про рівень послуг хмарних обчислень [19].

Що ж стосується спеціального регулювання, яке визначає порядок використання хмарних послуг безпосередньо у фінансовому секторі в ЄС, то серед важливих документів слід виокремити План дій фінтех (2018 р.), окремий розділ якого присвячено усуненню перепон на шляху використання хмарних послуг. У ньому звертається увага на необхідність стандартних контрактів між НХП і фінансовою установою, а також розв'язання таких питань, як аудит, вимоги щодо звітності й визначення, які функції можуть розглядатися як важливі під час передачі на аутсорсинг НХП. Також акцентується на необхідності розробки саморегулювальних міжгалузевих кодексів поведінки, щоб полегшити перехід від одного НХП до іншого [20, п. 2.2].

Спочатку законодавство щодо регулювання використання хмарних послуг було розроблено стосовно банківського сектору у 2017 р. [21] та удосконалено у 2019 р. [22], потім за його прикладом було розроблено й стосовно інших секторів фінансового ринку – страхового й пенсійного секторів (2020 р.) [23] і ринку капіталу (2021 р.) [24]. Фактично натепер питання використання хмарних послуг у фінансовому секторі врегульовані всіма європейськими регуляторами фінансового ринку – Європейським органом банківського нагляду (далі – ЕВА), Європейською організацією страхування та пенсійного забезпечення (далі – ЕІОРА) та Європейським

органом із цінних паперів і ринків (далі – ESMA). Мета регулювання в усіх секторах фінансового ринку однакова: протидіяти ризикам і сприяти належному нагляду під час переходу на хмарні технології. Слід зазначити, що критерії щодо регулювання хмарних послуг в усіх секторах також однакові. У Керівництві ESMA прямо зазначається, що за основу регулювання було взято документи ЕВА та ЕІОРА, а також що ESMA має на меті досягти єдиного підходу щодо регулювання хмарних послуг із тими, що існують в інших секторах [25, с. 2].

Передача обробки даних надавачу хмарних послуг розглядається як *форма ІТ аутсорсингу*, тому до нього застосовуються загальні правила щодо регулювання аутсорсингу. Однак через специфіку аутсорсингу хмарних технологій у фінансовому секторі до нього застосовується специфічне регулювання, що є продовженням загального регулювання щодо аутсорсингу й ураховує специфіку хмарних технологій у фінансовому секторі. ESMA визнає, що в порівнянні з більш традиційними формами аутсорсингу ІТ, хмарні послуги, як правило, більш стандартизовані й надаються клієнтам у високо автоматизованому порядку й у великому обсязі [25, п. 1, с. 3].

Особливістю регулювання використання хмарних технологій в ЄС є його спрямування на регулювання аутсорсингу *критичних або важливих функцій*. ESMA відносить до них «будь-яку функцію, дефект або збій у виконанні якої суттєво погіршить:

- а) дотримання установою своїх зобов'язань відповідно до чинного законодавства;
- б) фінансові показники діяльності установи;
- в) надійність або безперервність надання основних послуг і видів діяльності установи» [24, с. 7].

ЕВА окрім зазначених критеріїв установлює ще додаткові для визначення критичних або важливих функцій [22, п. 29].

Регулювання щодо всіх секторів фінансового ринку в ЄС охоплює такі питання:

- 1) вимоги до системи управління, документації та обов'язок фінансової установи повідомляти орган нагляду про передачу критичних або важливих функцій на аутсорсинг НХП;
- 2) дью дїлідженс надавача хмарних послуг;
- 3) договір про надання хмарних послуг;
- 4) субаутсорсинг;
- 5) моніторинг та оверсайт діяльності надавача хмарних послуг і його аудит;
- 6) припинення користування хмарними послугами;
- 7) нагляд за надавачами хмарних послуг.

Слід зазначити, що підхід до регулювання однаковий щодо всіх типів фінансових установ, розрізняється лише ступінь деталізації регулювання – найширшим є регулювання ЕВА, далі – ЕІОРА й нарешті – ESMA.

Вимоги до системи управління, документації та обов'язок фінансової установи повідомляти органу нагляду про передачу критичних або важливих функцій на аутсорсинг НХП містять обов'язковість наявності стратегії (політики) передачі на аутсорсинг функцій НХП, вимоги до якої чітко регламентовані, й внутрішні

політики й процеси, включаючи щодо ІКТ, інформаційної безпеки й операційного ризик-менеджменту. Також встановлено обов'язок фінансових установ повідомляти орган нагляду про передачу критичних або важливих функцій на аутсорсинг НХП [22, гл. 3; 23, п. 12–18, п. 44–45; 24, п. 17–26].

Передбачено обов'язкове проведення *аналізу, що передує аутсорсингу, і дью ділідженс* до передачі фінансовою установою критичних або важливих функцій на аутсорсинг НХП. По-перше, фінансова установа має оцінити всі ризики такої запланованої передачі, а також вигоди й витрати, які можуть виникати за такої умови. По-друге, дью ділідженс має проводитися до передачі НХП фінансовою установою її функцій на аутсорсинг, а в певних випадках додатково й після такої передачі (коли фінансова установа дізналася про значні недоліки чи зміни в послугах, що надаються НХП), і передбачається, що дью ділідженс має розглядати, чи підходящий НХП, а також низку інших чинників, які мають братися до уваги під час його проведення, такі як безпека НХП та інші. Загалом регулювання всіх типів фінансових установ подібне, є лише незначна відмінність у чинниках, які мають братися до уваги під час проведення дью ділідженс [22, гл. 12, 12.3; 23, п. 27, 33–35; 24, п. 19–25].

Чітко визначені істотні умови *договору про надання хмарних послуг* із метою забезпечення надійного захисту фінансових установ, що передають критичні або важливі дані, на аутсорсинг НХП. Вони містять: фінансові обов'язки фінансової установи й НХП; право, яке застосовується до цього договору; чи дозволяється субаутсорсинг та якщо так, то на яких умовах; місцерозташування даних, які мають зберігатися НХП; питання забезпечення конфіденційності даних і безпеки послуг, що надаються НХП; його звітування; право фінансової установи на моніторинг і наглядового органу на здійснення нагляду за діяльністю НХП, включаючи аудит, щодо функцій, переданих на аутсорсинг та інше [22, гл. 13; 23, п. 36–37; 24, п. 26–28].

У випадку, якщо *субаутсорсинг критичних або важливих функцій* допускається, то передбачається, що завчасно має бути визначено, на яких умовах він дозволяється, які функції не можуть передаватися на аутсорсинг; НХП має залишатися відповідальним щодо функцій, переданих на субаутсорсинг; обов'язковість повідомлення фінансової установи про намір передати певні функції на субаутсорсинг і можливість фінансової установи виступати проти субаутсорсингу або його допустимість лише після попереднього погодження фінансовою установою та інше [22, гл. 13.1; 23, п. 50; 24, п. 42–43].

Особлива увага приділяється забезпеченню проведення *аудиту критичних або важливих функцій, переданих на аутсорсинг НХП*. Зокрема, законодавчо закріплено, що договір про аутсорсинг таких функцій НХП не може обмежувати право фінансової установи на аудит НХП; фінансова установа має право визначати частоту аудиту й сфери, що підлягають аудиту, залежно від ступеня їх ризику; також встановлені вимоги до порядку проведення аудиту НХП щодо функцій фінансової установи, які йому передані на аутсорсинг [22, гл. 13.3; 23, п. 38–46; 24, п. 34–41].

Порядок регулювання *припинення користування послугами НХП* у випадку, якщо йому були передані на аутсорсинг критичні або важливі функції НХП, дуже

важливий, адже можуть виникати ризики щодо можливості виконання фінансовими установами своїх основних функцій. Саме тому законодавці рекомендують мати стратегію виходу / припинення користування послугами НХП у випадку, якщо йому були передані на аутсорсинг критичні або важливі функції, а також визначити альтернативні рішення чи план переходу від одного НХП до іншого або повернення до здійснення зазначених функцій безпосередньо самою фінансовою установою. Регулювання щодо всіх типів фінансових установ подібне. На відміну від ESMA й ЕІОРА, ЕВА конкретизує перелік випадків, щодо яких фінансова установа повинна мати план виходу й план такого переходу, а саме у випадку припинення договору аутсорсингу, банкрутства НХП, погіршення якості наданої функції та фактичних чи потенційних перебоїв у бізнесі, спричинених неналежним забезпеченням або незабезпеченням функції; суттєвих ризиків, що виникають у процесі належного й безперервного застосування функції [22, п. 106].

Виокремлено здійснення *нагляду під час аутсорсингу функцій НХП* фінансовими установами з-поміж здійснення загального нагляду за діяльністю фінансових установ. Регламентовано порядок здійснення такого нагляду й передбачено застосування пропорційного підходу до його здійснення. Регулювання регуляторів ЄС щодо всіх типів фінансових ринків стосовно порядку нагляду подібне, однак ЕВА детально регламентує ширше коло ризиків, які підлягають оцінці під час здійснення нагляду. Якщо ESMA виокремлює лише концентраційний ризик [24, п. 49], то Керівництва ЕІОРА й ЕВА передбачають оцінку значного ширшого кола ризиків, окрім концентраційного, також операційного, репутаційного ризиків, ЕІОРА передбачає ризик ІКТ [23, п. 48], а ЕВА – також ризик необхідності надання фінансової допомоги НХП із тим, щоб уникнути його неплатоспроможності, конфліктів інтересів між кредитною установою та НХП та іншого [22, п. 116].

Слід зауважити, що в основу як регулювання, так і нагляду використання хмарних технологій у фінансовому секторі ЄС покладено **пропорційний підхід**. Пропорційний підхід під час регулювання полягає в застосуванні диференційованого підходу до регулювання критичних або важливих та інших функцій, спрямованого на врахування різного характеру ризику під час передачі цих функцій на аутсорсинг; детальне регулювання та вимоги встановлені лише щодо передачі на аутсорсинг критичних або важливих функцій НХП. Пропорційний підхід під час здійснення нагляду полягає в тому, що:

1) основний фокус нагляду має бути зосереджено на аутсорсингу критичних або важливих функцій;

2) орган нагляду під час здійснення своїх наглядових повноважень враховує обсяг і складність переданих функцій на аутсорсинг, а також ризики, що виникають внаслідок договору аутсорсингу, у тому числі такий специфічний ризик, як концентраційний [22; 23; 24].

Подальший розвиток регулювання хмарних послуг у фінансовому секторі передбачає:

1) розробку модельних умов договору на користування хмарними технологіями. Натепер відповідні ініціативи висунуті Європейською коаліцією хмарних користувачів (The European Cloud User Coalition (ECUC)). Так, зокрема, модельні

умови договору на користування хмарними технологіями мають передбачати повідомлення про будь-які зміни або припинення роботи хмарного сервісу принаймні за 18 місяців; НХП має здійснювати моніторинг і звітувати про показники ефективності й автоматизовані звітні відхилення без додаткової плати для фінансової установи; у договорі страхування має бути зазначено, що вартість страхового покриття має зростати зі збільшенням кількості активів у хмарі й інше [26];

2) розвиток законодавства щодо підвищення кібербезпеки у фінансовому секторі. Так, учені (Krüger, Brauchle (2021 р.)) пропонують розробити єдине регулювання протидії ризикам ІКТ і кібербезпеки щодо всіх фінансових установ; звернути увагу на системний характер кіберризиків, що може виникати внаслідок недотримання норм інформаційної безпеки [27, с. 4–5].

У Швейцарії питання аутсорсингу функцій НХП урегульовано в Циркулярі FINMA 2018/3 «Аутсорсинг – банки й страховики» щодо банків, страхових компаній і дилерів цінних паперів [28], а також Швейцарська банківська асоціація видала Керівництво щодо застосування цього Цирюляру [29]. Регулювання аутсорсингу функцій фінансових установ НХП подібне до законодавства ЄС. Однак у Швейцарії більше уваги приділяється питанням інформаційної безпеки, зберігання та обробки даних НХП (місцезоташування даних, порядку його зміни) і банківської таємниці; передача на аутсорсинг іноземному НХП допускається, якщо фінансова установа має можливість у будь-який час отримати доступ до будь-якої захищеної інформації, яка зберігається або обробляється за кордоном НХП, а також якщо допускається його безперешкодний аудит як внутрішніми й зовнішніми аудиторами, так і органом нагляду. Акцентується на обов'язку фінансової установи інформувати клієнтів, чи обробляються персональні дані в межах хмарних послуг. Цей обов'язок можна виконати шляхом включення відповідної інформації в політиці установи щодо захисту даних. В юридичній літературі також звертається увага на важливість розуміння рівня захисту персональних даних у країні, в якій вони зберігаються чи обробляються, залежно від його ступеня можуть бути необхідні додаткові заходи для забезпечення належного захисту персональних даних [30, с. 6].

У Сінгапурі теж передбачено подібні принципи регулювання передачі важливих функцій на аутсорсинг НХП. Важлива увага приділяється забезпеченню безпеки передачі цих функцій НХП. Чітко визначені права й обов'язки Ради директорів і старшого менеджменту в процесі аутсорсингу НХП. Також звертається увага на особливості передачі цих функцій іноземному НХП, така передача дозволяється за відсутності ризику країни, що передбачає наявність економічних, соціальних і політичних умов і подій в іноземній країні, що можуть негативно вплинути на установу. У випадку передачі важливих функцій на аутсорсинг іноземному НХП дью ділідженс має містити аналіз ризику країни. Також під час передачі важливих функцій на аутсорсинг іноземному НХП не мають створюватися перешкоди уповноваженому органу для здійснення ним нагляду за фінансовою установою [31, п. 5.10].

У Бразилії питання аутсорсингу критичних функцій фінансовими установами, ліцензованими Центральним банком Бразилії, врегульовані у виданому останнім

Положенні № 4658/2018, який визначає правила вступу в договірні відносини щодо хмарних обчислень, обробки й зберігання даних, а також політики кібербезпеки. Загальні засади регулювання хмарних обчислень у Бразилії схожі з аналізованим вище регулюванням в інших країнах. Цікавий порядок передачі зберігання даних і хмарних обчислень, наданий за кордоном; він допускається за умови:

а) наявності угоди про обмін інформацією між Центральним банком Бразилії та наглядовими органами країн, де можуть надаватися хмарні послуги;

б) надання послуг НХП має не завдавати шкоди функціонуванню фінансової установи й не перешкоджати діям Центрального Банку Бразилії;

в) до укладення договору мають бути визначені країни й регіони кожної країни, де можна надавати послуги й зберігати, обробляти дані;

г) НХП повинен передбачити альтернативи для забезпечення безперервності бізнесу в разі неможливості продовження ним договору або в разі його розірвання [32, п. 16].

Отже, європейський законодавець розглядає пріоритетність використання хмарних технологій, у тому числі й у фінансовому секторі, щодо широкого кола фінансових установ. Регулювання хмарних послуг здійснюється як на загальному, так і на спеціальному рівнях. Закладено єдиний підхід і загальні критерії щодо регулювання всіх типів фінансових установ. Правова підстава використання хмарних технологій – договір аутсорсингу. Ключовий принцип регулювання – принцип пропорційності; регулювання, головним чином, спрямоване на аутсорсинг критичних або важливих функцій НХП. Регулювання передачі функцій на аутсорсинг НХП в усіх секторах фінансового ринку подібне, лише незначні відмінності передбачені в регулюванні різних типів фінансових установ. Аналіз законодавства Швейцарії, Сінгапуру й Бразилії показав, що підхід до регулювання хмарних послуг у цих країнах базується на тих самих засадах, що й в ЄС, однак у цих країнах більше уваги приділяється регулюванню питання ризику країни й визначенню умов, за яких допускається передача функцій на аутсорсинг іноземному НХП, а також питанням інформаційної безпеки, зберігання та обробці даних НХП.

5. Висновки й рекомендації щодо моделі регулювання хмарних послуг в Україні

Ураховуючи те, що використання хмарних технологій у фінансовому секторі містить більше переваг у порівнянні з ризиками, які виникають від їх використання, українському законодавцеві рекомендується створити належну законодавчу основу, яка б забезпечила активне впровадження хмарних технологій і мінімізувала ризики, що виникають від їх використання. Рекомендується під час побудови моделі законодавчого регулювання хмарних послуг в Україні застосовувати комплексний підхід, який передбачає одночасну розробку як загального регулювання, що визначає основні засади регулювання хмарних послуг, так і спеціального, що визначає особливості надання цих послуг у певних сферах, зокрема таких, як фінансовий сектор. Вважаю, що такий підхід надасть можливість забезпечити єдність термінології та належний захист користувачів хмарних послуг.

Під час розробки загального законодавства щодо хмарних послуг мають бути встановлені стандарти діяльності НХП (рекомендується під час їх розробки враховувати положення Європейського хмарного кодексу поведінки (2021 р.), серти-

фікації їх діяльності й послуг, що ними надаються, і забезпечуватися належний нагляд за діяльністю НХП. Також мають бути створені основи як для допуску зарубіжних НХП із високою репутацією, так і для розвитку українських НХП із тим, щоб забезпечити створення конкурентного середовища у сфері хмарних послуг. Слід стимулювати інформаційну обізнаність про хмарні технології та про правові форми захисту під час їх користування.

Рекомендується українському законодавцеві слідувати практиці країн із розвиненими фінансовими ринками й законодавчо закріпити, що регулювання передачі функцій на аутсорсинг НХП має здійснюватися щодо всіх типів фінансових установ (як банківських, так і небанківських) і мати пропорційний характер (має бути, головним чином, спрямоване на аутсорсинг критичних або важливих функцій). Воно має охоплювати такі питання, як вимоги до системи управління, обов'язку фінансової установи повідомляти орган нагляду про передачу критичних або важливих функцій на аутсорсинг НХП; дью ділідженс НХП; договір про надання хмарних послуг, включаючи субаутсорсинг; моніторинг та аудит НХП; припинення користування хмарними послугами; нагляд за НХП. Пропонується розробити в Україні модельний договір про надання хмарних послуг фінансовим установам й стандарти проведення аудиту й здійснення ефективного нагляду компетентними органами. Важлива увага має приділятися ризику країни й особливо забезпеченню конфіденційності даних та інформаційної безпеки у фінансовому секторі України НХП.

Вважаю, що побудова ефективної моделі законодавчого регулювання використання хмарних технологій у фінансовому секторі позитивно позначиться на його розвитку й українській економіці загалом.

Література

1. Swiss Finance Council. Getting Ready for the 20s – Technology and the Future of the Global Banking. 2020. URL: https://www.swissfinancecouncil.org/images/SFC_Discussion_Paper_2020.pdf.
2. Poole A. Banking on the Cloud in the Face of COVID-19 and Beyond. 22 June 2020. *Fintech Futures*. URL: <https://www.fintechfutures.com/2020/06/banking-on-the-cloud-in-the-face-of-covid-19-and-beyond/>.
3. Capgemini. Cloud Computing in Banking. What Banks Need to Know When Considering a Move to the Cloud. 2011. URL: https://www.capgemini.com/wpcontent/uploads/2017/07/Cloud_Computing_in_Banking.pdf.
4. Yan G. Application of Cloud Computing in Banking: Advantages and Challenges. *2nd International Conference on Politics, Economics and Law*. 2017. Vol. 23. P. 29–32.
5. Crisanto J.C., Donaldson C., Ocampo D., Prenio J. FSI Insights on policy implementation. No 13. Regulating and supervising the clouds: emerging prudential approaches for insurance companies. December 2018. URL: <https://www.bis.org/fsi/publ/insights13.pdf>.
6. FSB. Third-party Dependencies in Cloud Services Considerations on Financial Stability Implications. 9 February 2019. URL: <https://www.fsb.org/wp-content/uploads/P091219-2.pdf>
7. Toronto Centre. Cloud Computing: Issues for Supervisors. URL: <https://res.torontocentre.org/guidedocs/Cloud%20Computing%20FINAL.pdf>.
8. Book A. How Cloud Computing is Contributing to the Exponential Growth of Tech in Emerging Markets. 13 February 2018. URL: <https://www.seedstars.com/content-hub/life/how-cloud-computing-contributing-exponential-growth-tech-emerging-markets/>.
9. AFME. The Adoption of Public Cloud Computing in Capital Markets. November 2019. URL: <https://www.pwc.co.uk/financial-services/assets/pdf/afme-cloud-paper-november-2019.pdf>.
10. FSB. BigTech Firms in Finance in Emerging Market and Developing Economies. Market developments and potential financial stability implications. 12 October 2020. URL: <https://www.fsb.org/wp-content/uploads/P121020-1.pdf>.

11. Стратегія розвитку фінтех в Україні до 2025 року. Липень 2020 року / Національний Банк України. URL: <https://bank.gov.ua/ua/files/DDWIAwXTdjdClр>.
12. Стратегія розвитку фінансового сектору України до 2025 р. (оновлена в березні 2021 р.) / Міністерство фінансів України, Національний Банк України, Національна Комісія, що здійснює державне регулювання у сфері ринків фінансових послуг, ФГВФО. URL: https://bank.gov.ua/admin_uploads/article/Strategy_FS_2025.pdf?v=4.
13. Про затвердження Національної економічної стратегії на період до 2030 року : Постанова Кабінету Міністрів України від 3 березня 2021 року № 179 / Кабінет Міністрів України. *Офіційний вісник України*. 2021. № 22. Ст. 1015.
14. Про хмарні послуги : Проект Закону України № 2655 від 20 грудня 2019 р. *База даних «Законодавство України»*. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67744.
15. European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Unleashing the Potential of Cloud Computing in Europe'. 2012. COM/2012/0529 final.
16. The EU Code of Conduct. 2021. URL: <https://eucoc.cloud/en/about/about-eu-cloud-coc/>.
17. CSPCERT WG. Recommendations for the Implementation of the CSP Certification Scheme. June 2019. URL: <https://www.enisa.europa.eu/news/enisa-news/cybersecurity-certification-lifting-the-eu-into-the-cloud>.
18. ENISA. Cybersecurity Certification EUCC, a Candidate Cybersecurity Certification Scheme to Serve as a Successor to the Existing SOG-IS. May 2021. URL: <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1>.
19. Cloud Service Level Agreement Standardisation Guidelines. 24 June 2014. URL: <https://digital-strategy.ec.europa.eu/en/news/cloudservice-level-agreement-standardisation-guidelines>.
20. European Commission. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action plan: For a more competitive and innovative European financial sector. Brussels, 8.3.2018 COM. 2018. 109 final.
21. EBA. Recommendations on Outsourcing to Cloud Service Providers. Final Report. 20 December 2017. EBA/REC/2017/03.
22. EBA. Guidelines on Outsourcing Arrangements. Final Report. 25 February 2019. EBA/GL/2019/02.
23. EIOPA. Guidelines on Outsourcing to Cloud Service Providers. 06 Feb 2020. EIOPA-BoS-20-002.
24. ESMA. Guidelines on Outsourcing to Cloud Service Providers. 10 May 2021. ESMA50-164-4285.
25. ESMA. Final Report Guidelines on outsourcing to cloud service providers. 18 December 2020. ESMA50-157-2403.
26. Coalition of European Banks Calls for Model Cloud Services Terms. June 2021. URL: <https://www.jdsupra.com/legalnews/coalition-of-european-banks-calls-for-7268493/>.
27. Krüger P.S., Brauchle J.P. The European Union, Cybersecurity, and the Financial Sector: A Primer. March 16, 2021. WP, Carnegie Endowment for International Peace. URL: https://carnegieendowment.org/files/Krueger_Brauchle_Cybersecurity_legislation.pdf.
28. FINMA. Circular 2018/3 Outsourcing – banks and insurers. 21 September 2017.
29. Swiss Bankers Association, Cloud Guidelines. A Guide to Secure Cloud Banking. June 2020. 2nd edition.
30. PwC. Taking Swiss Private Banking to the Cloud. 2018. URL: https://www.pwc.ch/en/publications/2018/Taking%20Swiss%20Private%20Banking%20to%20the%20Cloud_EN_web.pdf.
31. Monetary Authority of Singapore. Guidelines on outsourcing. 27 July 2016. URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Outsourcing-Guidelines_Jul-2016-revised-on-5-Oct-2018.pdf.
32. Central Bank of Brazil. Resoloton CMN 4,658. 26 April 2018. How Cloud Computing is Contributing to the Exponential Growth of Tech in Emerging Markets. URL: <https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf> (accessed: 1 August 2021).
33. IOSCO. Principles on Outsourcing Consultation Report. May 2020. CR01/2020.
34. Сопільник Л., Скриньковський Р., Віконський В., Ковалів М., Заяць Р., Єсімов С., Малашко О. Особливості правового забезпечення інформаційної безпеки при використанні хмарних технологій органами державної влади. *Traektorія Nauki = Path of Science*. 2020. Vol. 6. No 6. P. 5006–5013.

Анотація

Хорт Ю. В. Регулювання хмарних технологій у фінансовому секторі України. – Стаття.

Наразі у всьому світі відбувається стрімкий розвиток використання хмарних технологій у всіх сферах, включаючи фінансовий сектор. Однак у науковій літературі проблеми правового регулювання хмарних технологій у фінансовому секторі України не отримали належного висвітлення. Стаття присвячена аналізу переваг і ризиків щодо використання хмарних технологій у фінансовому секторі; дослідженню стану й підходів до їх регулювання як в Україні, так і за кордоном; наданню відповідних рекомендацій щодо побудови моделі законодавчого регулювання хмарних технологій у фінансовому секторі України. У статті доводиться, що вигоди від використання хмарних технологій у фінансовому секторі значно більші в порівнянні з ризиками від їх використання. Аналіз українського законодавства показав, що законодавець задекларував необхідність розвитку хмарних технологій. Однак законопроект України «Про хмарні послуги» містить низку недоліків і підлягає удосконаленню. Авторка пропонує застосовувати комплексний підхід моделі законодавчого регулювання хмарних послуг в Україні, який передбачає одночасну розробку як загального законодавства, що визначає основні засади регулювання хмарних послуг, так і спеціального законодавства, що визначає особливості надання цих послуг у певних сферах, зокрема у фінансовому секторі. Рекомендується українському законодавцеві слідувати практиці країн із розвиненими фінансовими ринками й законодавчо закріпити, що регулювання передачі функцій на аутсорсинг надавачам хмарних послуг має здійснюватися щодо всіх типів фінансових установ (як банківських, так і небанківських) і мати пропорційний характер (має бути, головним чином, спрямоване на аутсорсинг критичних або важливих функцій). Пропонується розробити в Україні модельний договір про надання хмарних послуг фінансовим установам і стандарти проведення аудиту й здійснення ефективного нагляду компетентними органами. Увага має приділятися врегулюванню ризику країни й особливо забезпеченню конфіденційності даних та інформаційної безпеки у фінансовому секторі України надавачами хмарних послуг.

Ключові слова: надавач хмарних послуг, хмарна послуга, хмарні обчислення, фінансова установа, фінтех.

Summary

Khort Yu. V. Regulation of cloud technologies in the financial sector of Ukraine. – Article.

Currently, rapid development of cloud technologies usage in all areas, including the financial sector, can be noticed. However, in scholarly literature, the problems of legal regulation of cloud technologies in the financial sector of Ukraine have not been reflected. This article examines the benefits and risks of using cloud technologies in the financial sector; conducts an analysis of the state and approaches to their regulation both in Ukraine and abroad and gives a range of recommendations for building a model of legislative regulation of cloud technologies in the financial sector of Ukraine. This article argues that the benefits of using cloud technologies in the financial sector far outweigh the risks of using them. An analysis of Ukrainian legislation has shown that the lawmaker has declared the need to develop cloud technologies. However, the Draft of Law of Ukraine “On Cloud Services” has a number of shortcomings and requires improvement. The author suggests that the model of the legislative regulation of cloud services in Ukraine should be based on an integrated approach, which involves the simultaneous development of both general legislation defining the basic principles of cloud services regulation and special legislation defining the specifics of these services in certain areas, in particular, in the financial sector. This study recommends for the Ukrainian legislator to follow the practice of countries with developed financial markets and envisage the possibility of outsourcing of functions to the cloud service providers for all types of financial (both banking and non-banking) institutions and application of the proportionate regulatory approach (mainly aiming to outsource of critical or important functions). The author also suggests developing in Ukraine a model contract for the provision of cloud services to the financial institutions and standards for auditing and effective supervisory practices exercised by competent authorities. Mitigation of country risk and especially providing data confidentiality and information security in the financial sector of Ukraine by cloud service providers deserve particular attention.

Key words: cloud service provider, cloud service, cloud computing, financial institution, fintech.