USAID | UKRAINE
FROM THE AMERICAN PEOPLE

ПРОЕКТ З ТОРГОВЕЛЬНОЇ ПОЛІТИКИ

Основні тенденції правового регулювання у сфері електронної комерції

15 лютого 2017 року
Ця публікація була підготовлена International Group Development LLC, для розгляду Агентством США з міжнародного розвитку.

ПРОЕКТ З ТОРГОВЕЛЬНОЇ ПОЛІТИКИ

Основні тенденції правового регулювання у сфері електронної комерції

«Основні тенденції правового регулювання у сфері електронної комерції» - публікація, підготовлена паном Сімеоном Сагайдачним – провідним експертом проекту USAID з торговельної політики в Україні. Мета публікації полягає в тому, щоб допомогти Урядові України та іншим зацікавленим сторонам у вивченні ключових питань і тенденцій у сфері регулювання електронної комерції під час подальшого наближення законодавчої бази України до права ЄС у цій сфері та гармонізації її з іншими міжнародними стандартами.

ЗМІСТ

Вступ 4
Частина I. Фундаментальні аспекти правової бази для електронної комерції 4
A. Ключові принципи 4
B. Сфера застосування 5
C. Міжнародні правові акти та стандарти 6
D. Основні терміни 7
E. Виконання традиційних вимог в електронному середовищі 7
Вимоги щодо письмової форми 8
Вимоги щодо підпису 8
Оригінал документа 8
Допустимість і доказова сила інформації 8
Збереження інформації 9
F. Електронні підписи 9
Еволюція законодавства в сфері електронного підпису 9
Основні законодавчі положення, що стосуються електронного підпису 11
Прийняття підписів шляхом натискання комп'ютерної миші 11
Нотаріальне засвідчення 12
G. Питання, пов'язані з передачею повідомлень 12
Атрибуція повідомлень даних 12
Підтвердження отримання 13
Час відправлення та отримання 13
Місце відправлення та отримання 14
Небажані повідомлення 14
H. Укладання договорів в сфері електронної комерції 15
Укладання договору 15
Вимоги щодо форми 16
«Битва форм» 16
Можливість виправлення помилок 16
Розкриття інформації 17
Включення шляхом посилання 17
Електронні ліцензійні угоди 17
I. Постачальники проміжних послуг 18
Вимоги щодо розкриття інформації 18
Режим відповідальності для постачальників проміжних послуг 18
J. Застосовність по відношенню до державних органів 19
Частина II. Додаткові питання, що стосуються правової бази електронної комерції 21
A. Оборотні документи 21
B. Мобільні гроші 24
Основи 24

Бізнес-моделі, що використовують м-гроші 25
Користувачі м-грошей 26
Ризики та заходи безпеки 29
Регуляторний підхід 33
C. Захист прав споживачів 35
D. Врегулювання суперечок 37

Вступ

1. У цьому документі наводиться загальний огляд ключових питань і тенденцій правового регулювання у сфері електронної комерції. Наведений огляд має на меті зорієнтувати Уряд України та інші зацікавлені сторони щодо деяких ключових питань і тенденцій, які мають бути розглянуті для подальшого наближення законодавчої бази України у сфері електронної комерції до права ЄС, та гармонізації її з іншими міжнародними стандартами.

2. Цей документ складається з двох основних частин. У першій частині наводиться огляд основних питань, які зазвичай регулюються в законі про електронну комерцію. У другій частині висвітлюється ряд додаткових питань, які можуть бути передбачені в законі про електронну комерцію та/або, можливо, в тій чи іншій мірі, в інших законодавчих актах. Незважаючи на те, що в цьому документі розглядаються різні теми і проблеми, а також різні акти ЄС та інші міжнародні документи, він, через обмежений обсяг завдання, не претендує на вичерпність в плані тематики, яка в ньому розглядається, або рекомендацій, які можуть бути отримані в результаті ознайомлення з ним.

Частина I. Фундаментальні аспекти нормативно-правової бази для електронної комерції

A. Ключові принципи

3. *Недискримінація* – основоположний принцип, який полягає в тому, що інформація не може бути позбавлена властивостей юридичної сили, чинності або застосування лише на тій підставі, що вона складена в електронній формі.[1]

4. *Право сторін укладати угоди* - нормативно-правова база електронної комерції в цілому повинна поважати право сторін укладати угоди, в яких вони домовляються про те, в якій спосіб вони будуть співпрацювати щодо умов обміну інформацією та документального оформлення угод.[2] Це включає в себе поняття згоди на використання електронних засобів. Така згода може бути прямою або випливати з поведінки.

5. *Електронні функціональні еквіваленти* - замість усунення існуючих правових понять і процедурних вимог, які традиційно застосовуються у торгівлі,

[1] Базується на Типовому законі про електронну торгівлю Комісії Організації Об'єднаних Націй з права міжнародної торгівлі (ЮНСІТРАЛ) (далі – "UMLEC"), стаття 5.
[2] UMLEC, стаття 4; UNCEC, стаття 3.

законодавство у сфері електронної комерції, як правило, встановлює способи задоволення цих традиційних вимог за допомогою еквівалентних електронних процедур.

6. *Технологічна нейтральність* - правове регулювання, що створює сприятливі умови для розвитку електронної комерції, не провинне нав'язувати або обмежувати основні принципи та процедури з використанням будь-якого конкретного технологічного рішення за рахунок виключення інших. Наприклад, законодавче визнання електронних підписів не повинне обмежуватись будь-якою конкретною технологічною формою, наприклад, цифровими підписами.

B. Сфера застосування

7. Залежно від підходу, прийнятого розробниками законодавства в цій галузі, сфера застосування закону про електронну комерцію може обмежуватись угодами комерційного характеру. З іншого боку, законодавство може мати більш широкі рамки, не обмежуючись угодами лише комерційного характеру (наприклад, закон може також охоплювати угоди і взаємодії між громадянами і урядом, або між урядовими або державними органами).

8. Закони про електронну комерцію зазвичай вилучають обмежене коло видів угод зі своєї сфери застосування. Приклади винятків включають договори, укладені в особистих, сімейних або домашніх цілях, операції на регульованих біржах, передачу прав на нерухоме майно, питання, що стосуються податків; скасування або припинення комунальних послуг. Можна відзначити, що якщо застосування законодавства у сфері електронної комерції ґрунтується на згоді сторін, число винятків може бути зменшене.[3]

9. До таких винятків також належать обігові документи (наприклад, документи про передачу, володіння якими дає їх власнику право вимагати доставки товару або виплати певної грошової суми, такі як транспортні накладні, векселі тощо).

10. Згодом практика виключення обігових документів, ймовірно, буде трохи менш звичайною, оскільки вже розпочався процес вироблення комерційних практик та відповідних правових підходів, які дозволяють дематеріалізацію обігових інструментів.[4]

11. Деякі акти на регіональному або міжнародному рівні, що стосуються питань електронної комерції, передбачають можливість держави в особливих випадках

[3] Див. UNCEC, стаття 2; Директиву ЄС про електронну комерцію, стаття 2.5; Уніфікований закон про електронні транзакції, розділ 3.

4 Див. роботу, яка зараз виконується ЮНСІТРАЛ з розробки Типового закону про електронні обігові документи.

відступати від правил, які зазвичай застосовуються. Наприклад, Директива ЄС про електронну комерцію [5] передбачає таку можливість щодо обмеженого кола випадків (наприклад, важливі питання державної політики, зокрема розслідування кримінальних справ, охорони здоров'я, захисту прав споживачів).

C. Міжнародні стандарти та правові акти

12. Серед міжнародних стандартів та правових актів, що закріплюють кращі підходи до регулювання в галузі електронної комерції, доцільно окреслити такі:

(a) Типовий закон про електронну торгівлю Комісії Організації Об'єднаних Націй з права міжнародної торгівлі (ЮНСІТРАЛ - UMLEC)[6]
(b) Типовий закон ЮНСІТРАЛ про електронні підписи (UMLES)[7]
(c) Різні директиви та регламенти ЄС
    a. про електронну комерцію[8]
    b. про електронну ідентифікацію та засвідчувальні сервіси (електронний підпис)[9]
    c. про захист персональних даних[10]
    d. про захист прав споживачів[11]
    e. про електронне інвойсування[12]
    f. про платіжні послуги (PSD2)[13]

---

5 Стаття 3.4.

6 http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

7http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html

8 Директива 2000/31/ЄС Європейського Парламенту і Ради ЄС від 8 червня 2000 року про деякі правові аспекти інформаційних послуг, в тому числі електронної комерції, на внутрішньому ринку, доступна на http://ec.europa.eu/internal_market/e-commerce/directive_en.htm (далі – "Директива ЄС про електронну комерцію").

9 Регламент Європейского Парламенту і Ради ЄС 910/2014 від 23 липня 2014 року про електронну ідентифікацію та засвідчувальні сервіси для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС, доступний на http://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

10 Регламент Європейского Парламенту і Ради ЄС 2016/679 від 27 квітня 2016 року про захист фізичних осіб при обробці персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЕС (Регламент про загальний захист даних), доступний на http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

11 Директива 2011/83/ЄС Європейського парламенту і Ради ЄС від 25 жовтня 2011 року про права споживачів, що вносить зміни до Директиви 93/13/ЄЕС та Директиви 1999/44/ЄС Європейського парламенту і Ради ЄС і скасовує Директиву 85/577/ ЄЕС та Директиву 97/7/ЄС Європейського парламенту і Ради ЄС; доступна на http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&rid=1.

12 Директива 2014/55/ЄС Європейського парламенту і Ради ЄС від 16 квітня 2014 року про електронне інвойсування в державних закупівлях, доступна на http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0055&from=EN.

(d) Конвенція ООН про використання електронних повідомлень в міжнародних договорах (UNCEC)[14]
(e) Уніфікований закон про електронні транзакції (UETA – США)[15]
(f) Закон про електронні підписи в міжнародних і внутрішньодержавних торговельних відносинах (ESIGN – США)[16]

D. Основні терміни

13. Приклади основних термінів, які широко використовуються в міжнародній практиці, включають:

«Повідомлення даних» – інформація, підготовлена, відправлена, отримана або що зберігається за допомогою електронних, оптичних або аналогічних засобів, включаючи електронний обмін даними (ЕОД), електронну пошту, телеграму, телекс або телефакс [17] . Альтернативні терміни, що використовуються на практиці, включають «електронне повідомлення», «електронний запис» і «електронний документ». У деяких нормативно-правових актах розрізняють терміни «повідомлення даних» і «повідомлення» або «електронне повідомлення», при цьому два останніх терміна прив'язані конкретно до укладання договорів.[18]

«Посередник» відносно до конкретного повідомлення даних означає постачальникуа послуг, який від імені одержувача послуг відправляє, отримує або зберігає це повідомлення даних або надає інші послуги стосовно цього повідомлення даних.[19]

E. Виконання традиційних вимог в електронному середовищі

14. Без відмови від традиційних формальних вимог (наприклад, письмова форма, подання оригіналу документа, підпис, зберігання документів), законодавство у сфері електронної комерції, як правило, передбачає можливість їх виконання за допомогою електронних функціональних еквівалентів, як зазначено нижче.

---

13 Директива (ЄС) 2015/2366 Європейського парламенту та Ради ЄС від 25 листопада 2015 року про платіжні послуги на внутрішньому ринку, що вносить зміни до Директив 2002/65/ЄС, 2009/110/ЄС та 2013/36/ЄС та до Регламенту (ЄС) 1093/2010, та скасовує Директиву 2007/64/ЕС; доступна на http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN.
[14] http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.
[15] http://www.uniformlaws.org/Act.aspx?title=Electronic%20Transactions%20Act.
[16] https://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf.
[17] UMLEC, стаття 2(a).
[18] UNCEC, стаття 4(b).
[19] UMLEC, стаття 2(e).

Вимоги щодо письмової форми

15. Законодавство у сфері електронної комерції повинне передбачати, щоб інформація була надана у письмовій формі. Ця вимога вважається виконаною за умови дотримання певних умов (тобто, інформація в електронній формі повинна бути доступною для її подальшого використання).[20]

Вимоги щодо підпису

16. Законодавство у сфері електронної комерції повинне передбачати, щоб інформація була засвідчена (тобто підписана). Ця вимога вважається виконаною за допомогою функціонального еквіалента підпису за умови використання належного способу ідентифікації особи та зазначення факту згоди цієї особи з інформацією.

Оригінал документа

17. Законодавство у сфері електронної комерції повинне передбачати, щоб інформація надавалась або зберігалась в її оригінальній формі. Ця вимога вважається виконаною із застосуванням електронних засобів за умови, що існують надійні докази цілісності інформації з моменту, коли вона була підготовлена в її остаточній формі (повнота та незмінність змісту інформації) та що ця інформація може бути продемонстрована особі, якій вона повинна бути перед'явлена.[21]

Допустимість і доказова сила інформації

18. У правових системах, де це було б корисно зробити, нормативно-правова база має підтвердити, що жодні положення норм доказового права не застосовуються таким чином, щоб заперечувати допустимість інформації в якості доказу лише на тій підставі, що вона являє собою електронне повідомлення, та що їй буде надано належну доказову силу (з урахуванням відповідних міркувань, наприклад, надійності способу, за допомогою якого забезпечувалась цілісність інформації, способу, за допомогою якого був ідентифікований її розробник, і будь-яких інших відповідних факторів).[22]

[20] UMLEC, стаття.6.

[21] UMLEC, стаття 8.

[22] UMLEC, стаття 9.

Збереження інформації

19. Законодавство у сфері електронної комерції повинне передбачати збереження певних документів, записів або інформації в електронній формі за умови дотримання певних вимог (доступність для подальшого використання, точне представлення отриманої інформації, збереження інформації, яка дозволяє встановити походження та призначення інформації, а також дату і час її отримання.).[23] Положення щодо збереження інформації не поширюються на випадки, єдиною метою яких є зробити можливим відправлення чи отримання такої інформації.[24]

F. Електронні підписи

Еволюція законодавства в сфері електронного підпису

20. З початку впровадження законодавчих норм щодо електронних підписів було прийнято три види законів у цій сфері.[25] Перші законодавчі акти характеризувалися «технологічною ексклюзивністю», в якій конкретна технологічна форма електронного підпису (а саме електронного цифрового підпису) отримала юридичне визнання. У Сполучених Штатах, цю первісну групу законів уособлював Закон штату Юта про цифровий підпис (Utah Code Ann. § 46-3-101), після чого аналогічні закони були прийняті в Німеччині, Італії, Малайзії та Росії.

21. Друга хвиля, яку Блайт називає «технологічною нейтральністю», в якості реакції на вузькість підходу технологічної ексклюзивності, змінила технологічну обмеженість на користь відкритого підходу, який визнає різні види електронного підпису. Це включає в себе технологічно нейтральні мінімальні стандарти, які допускають будь-яку форму електронного підпису, яка відповідає цим стандартам. Наприклад, положення Типового закону ЮНСІТРАЛ про електронну комерцію, в якому йдеться про підпис (стаття 7), передбачає наступне:

> «(I) Якщо законодавство вимагає наявності підпису особи, ця вимога вважається виконаною стосовно повідомлення даних, якщо:

---

[23] UMLEC, стаття 10.

[24] UMLEC, стаття 10(2); проте, ані UETA, ані ESIGN не слідують Типовому закону ЮНСІТРАЛ (стаття 10(1)(c)) в частині вимог щодо можливості встановити походження та призначення інформації, а також дату і час її отримання.

[25] Див. Стівен Блайт (Stephen E. Blythe), “China’s New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce”, 7 Chicago-Kent Journal of Intellectual Property (2007), стор. 1-32. http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan041019.pdf. Автор зобов'язаний Блайту за цю розбивку законодавства у сфері електроннго підпису на три «хвилі».

(a) використовується будь-який спосіб для ідентифікації цієї особи та засвідчення того, що ця особа погоджується з інформацією, що міститься в повідомленні даних; та

(b) цей спосіб є настільки надійним, наскільки це відповідає цілі, для якої повідомлення даних було підготовлено чи передано з урахуванням всіх обставин, включаючи будь-які відповідні домовленості».

22. Третя хвиля законодавчих актів характеризується технологічно гібридним або дворівневим підходом. На одному рівні встановлюється технологічно нейтральний, мінімальний стандарт, який відкритий для різних різних типів електронних підписів. На другому рівні встановлений більш жорсткий стандарт, який за умовами та за характерними продуктами називається «вдосконаленим» або «безпечним», або «кваліфікованим» електронним підписом[26], і який, як правило, пов'язаний з «електронним цифровим підписом», та вважається таким, що має підвищену надійність (наприклад, «кваліфікований підпис» в Директиві ЄС про електронні підписи).

23. У законодавстві різних держав використання певного типу безпечного, вдосконаленого або кваліфікованого підпису може вимагатися для засвідчення автентичності окремих типів електронних документів (наприклад, в якості заміни для власноручного підпису на деяких типах документів, що в деяких випадках може вимагатися як доказ існування договору, укладеного за допомогою електронних засобів зв'язку).

24. Типовий закон ЮНСІТРАЛ про електронні підписи підтримує такий підхід, але до певної межі базується на технологічно нейтральному підході, що міститься у Типовому законі ЮНСІТРАЛ про електронну комерцію. Типовий закон про електронні підписи (стаття 3) підтверджує рівне ставлення до всіх підписних технологій (технологічна нейтральність). У тому ж ключі, як і положення про підпис в Типовому законі про електронну комерцію, Типовий закон про електронні підписи (стаття 6.1) передбачає, що вимога про підпис, введена законом, задовольняється за рахунок електронного підпису, «який є настільки надійнім, наскільки це відповідає цілі, для якої повідомлення даних було підготовлено чи передано з урахуванням всіх обставин, включаючи будь-які відповідні домовленості».

25. Для того, щоб допомогти сторонам угоди у визначенні достатньо надійної форми електронного підпису в кожному конкретному випадку (а також окремим особам під час розгляду фактів в ході судового процесу), Типовий закон про

[26] Регламент ЄС про електронну ідентифікацію та засвідчувальні сервіси для електронних транзакцій встановлює трирівневу систему, що складається з електронного підпису першого рівня, другого рівня (вдосконалений електронний підпис) і третього рівня (цифрові підписи на основі «кваліфікованого сертифіката»).

електронні підписи передбачає набір критеріїв для визначення ступеня надійності відповідного варіанта електронного підпису в залежності від застосовної мети повідомлення даних, що підписується.

Важливо враховувати потреби малих і середніх підприємств, які можуть бути ігноровані, якщо система фокусується в основному на дорогих, технічно складних рішеннях.

Основні законодавчі положення, що стосуються електронного підпису

26. Нижче наведено перелік основних питань, що розглядаються в рамках законодавства про електронну комерцію, які стосуються електронних підписів.

(a) Визначення термінів, які використовуються в положеннях про електронні підписи;
(b) Твердження про те, що електронні підписи задовольняють юридичним вимогам до проставлення підписів, за умови виконання вимог щодо ідентифікації особи, яка поставила свій підпис, і затвердження нею підписаної інформації;
(c) Положення, що стосуються використання електронних підписів державними органами або дозволу на врегулювання нормативних питань щодо використання електронних підписів державними органами;
(d) Вимоги, які мають бути виконані для отримання статусу безпечного/ вдосконаленого/кваліфікованого підпису, в тому числі критерії, що застосовуються при визначенні комерційної обґрунтованості процедур безпеки, узгоджених сторонами для перевірки підпису в якості способу досягнення безпечного/вдосконаленого/кваліфікованого статусу для електронного підпису;
(e) Презумпція надійності, пов'язана з безпечним/вдосконаленим/ кваліфікованим електронним підписом;
(f) Положення про інфраструктуру сервісів електронного підпису (наприклад, «інфраструктура відкритого ключа») та процедури:
    a. обов'язки і функції сертифікаційних органів, що видають сертифікати електронного підпису;
    b. необхідний зміст сертифікату цифрового підпису;
    c. акредитація та регулювання діяльності сертифікаційних органів;
    d. визнання сертифікатів електронних підписів, виданих іноземними сертифікаційними органами.

Прийняття підписів шляхом «наснути, щоб прийняти»

27. Однією з поширених форм миттєвого надання згоди в режимі онлайн є натискання (клік) – спосіб, в який укладається багато угод в електронній формі

через Інтернет. Варто зазначити, що коментар 7 до частини 2 UETA стверджує, що визначення терміна «електронний підпис» включає в себе «стандартний процес натискання відвідувачем веб-сторінки за посиланням». Можна відзначити, що відповідно до нормативних документів, таких як Конвенція Організації Об'єднаних Націй (стаття 9.3) і Директива ЄС про електронний підпис (стаття 2.1), для того, щоб натискання (клік) вважалося електронним підписом, воно повиненне бути ідентифікатором особи, що ставить свій підпис. (Див. також обговорення «електронних» угод в розділі I.G нижче).

Нотаріальне засвідчення

28. Різні країни мають різну практику нотаріального засвідчення електронних документів. UETA (розділ 11), відповідно до принципу функціональної еквівалентності, передбачає можливість використання електронного підпису нотаріуса (або іншої уповноваженої посадової особи) для нотаріального засвідчення, підтвердження, завірення або підтвердження під присягою підпису або документа.

G. Питання, пов'язані з передачею повідомлень

29. Різні питання, що стосуються передачі інформації, повинні бути врегульовані в законодавстві про електронну комерцію, як описано нижче.

Атрибуція повідомлень даних

30. Законодавство у сфері електронної комерції повинне встановити основні правила для атрибуції передачі інформації по відношенню до відправника повідомлення.

- ✓ Такі правила охоплюють ситуації, в яких повідомлення даних вважається повідомленням даних відправника, або коли адресат має право розглядати повідомлення як таке, що було отримано від відправника (відправлено особою, уповноваженою відправником, або відправлено інформаційною системою, запрограмованою відправником або від його імені, або відповідно до застосування адресатом узгодженої процедури перевірки);

- ✓ Такі правила також визначають умови, при яких адресат не має права вважати повідомлення даних повідомленням даних відправника (коли одержувач отримав своєчасне повідомлення від відправника про те, що повідомлення не було повідомленням відправника, або коли адресат не

виявив розумну обачливість або не використав узгоджену процедуру перевірки).[27]

Підтвердження отримання

31. Інше важливе питання, визначене законодавством у сфері електронної комерції, стосується підтвердження адресатом отримання повідомлення даних - в ситуації, коли відправник попросив адресата підтвердити отримання цього повідомлення даних або домовився з ним про таке підтвердження, і в ситуації, коли сторони не домовилися про будь-яку конкретну форму або спосіб підтвердження.[28]

Час відправлення та отримання

32. Так само, як в традиційному, паперовому середовищі, так і в електронному/кіберсередовищі, важливо встановити правила для визначення часу та місця відправлення та отримання повідомлення даних.[29]

- ✓ Що стосується часу відправлення повідомлення даних, ключовим фактором є момент часу, коли повідомлення даних надійшло в інформаційну систему поза контролем відправника (або представником відправника).

- ✓ Що стосується часу отримання, якщо адресат вказав інформаційну систему для отримання, то вважається, що отримання повідомлення мало місце, коли повідомлення даних надійшло у цю систему (що в деяких нормативно-правових документах сформульовано як момент часу, коли адресат отримав доступ до повідомлення).[30]

---

[27] UMLEC, стаття 13

[28] UMLEC, стаття 14.

[29] UMLEC, стаття 15; Директива ЄС про електронну комерцію не містить положення про час відправлення та отримання.

[30] Як можна побачити з підходу UETA, можливі додаткові уточнення щодо правил для визначення часу відправлення та часу отримання. Наприклад, зазначається, що для того, щоб відправка повідомлення мала місце, електронний документ повинен бути належним чином адесований або іншим належним чином направлений в інформаційну систему одержувача (розділ 15(a)(1)), а відправлений документ повинен бути у форматі, який здатна обробити система, в якій він повинен бути отриманий одержувачем (розділ 15(a)(2)). Крім того, хоча в цьому формулюванні, так само, як і в Типовому законі, йдеться про надходження документу в інформаційну систему, яка знаходиться поза контролем відправника, положення UETA стосується альтернативної можливості надходження повідомлення в «область системи обробки інформації, визначену або використовувану одержувачем, яка знаходиться під контролем одержувача». Мета цього нюансу полягає у вирішенні питання сценарію внутрішнього одержувача (наприклад, в університеті або корпорації), в якому повідомлення не може залишити інформаційну систему

Місце відправлення та отримання

33. Правила за умовчанням (оскільки сторони можуть змінити їх згідно зі своїм правом укладати угоди), що регулюють місце відправлення та отримання, як правило, сформульовані за наступними критеріями:

- ✓ місце, з якого повідомлення даних вважається відправленим, визначається виходячи з місця знаходження комерційного підприємства відправника (або місця знаходження комерційного підприємства, яке має безпосереднє відношення до основної транзакції, якщо відправник має декілька комерційних підприємств, або звичайне місце проживання відправника, якщо відправник не має комерційного підприємства);

- ✓ місцем, в якому повідомлення даних вважається отриманим, є місце знаходження комерційного підприємства адресата (або місце знаходження комерційного підприємства адресата, яке має безпосереднє відношення до основної транзакції, якщо адресат має декілька комерційних підприємств, або звичайне місце проживання адресата, якщо адресат не має комерційного підприємства);

- ✓ з точки зору визначення поняття «місце знаходження», місце знаходження обладнання та технічних засобів, що підтримують інформаційну систему, яка використовується будь-якою стороною для укладання угоди, або в якому інформаційна система може бути доступна для інших сторін, не залежить від місця розташування комерційного підприємства будь-якої сторони або звичайного місця проживання.[31]

Небажані повідомлення

34. Положення, що регулюють небажані повідомлення, є частиною комплексу положень, що становлять правову основу для електронної комерції - як відображено в праві ЄС, що регулює електронну комерцію.[32] Основний принцип,

---

відправника з технічної точки зору. Правило про момент отримання так само містить трохи більше нюансів, ніж формулювання в Типовому законі ЮНСІТРАЛ, зокрема, вимагаючи, щоб документ був отриманий інформаційною системою одержувача у формі, яка може бути оброблена цією системою (розділ15 () (2)). Інші особливості, зазначені в положеннях UETA, включають наступне: правила щодо отримання застосовуються навіть якщо інформаційна система одержувача фізично знаходиться в місці, відмінному від місця, в якому повідомлення вважається отриманим для юридичних цілей. (розділ 15(c)), як у Типовому законі (розділ 15(3)), і що електронний документ вважається отриманим, навіть якщо жодній особі не відомо про його отримання (розділ 15(e)).

[31] Див., наприклад, UNCEC, стаття 6.4.

[32] Див. зноску 11 вище.

втілений в таких положеннях, полягає в тому, що принаймні одержувачі повинні мати можливість відмовитися від отримання таких повідомлень.

H. Укладання договорів в сфері електронної комерції

Сфера застосування положень електронного договору

35. Попри те, що надання права на укладання договорів покладено в основу законодавства у сфері електронної комерції, можуть бути деякі винятки із загального підходу до укладання електронних договорів. Наприклад, не рідко такими винятками є договори, пов'язані із встановленням або передачею прав на нерухоме майно, а також договори, що регулюються сімейним правом.[33]

Укладання договору

36. Як і традиційні договори, що укладаються на папері, договори в сфері електронної комерції укладаються шляхом обміну оферти і акцепту (тобто, коли воля і наміри продавця та покупця збігаються). Нормативно-правова база для електронної комерції, як правило, містить різні положення, які дозволяють укладання договорів в режимі онлайн.

37. Типи положень, що описані вище (розділи I, E та F), дозволяють безпаперовий обмін оферти і акцепту. Вони дозволяють виконання нормативних вимог про те, що договір повинен бути укладений в письмовій формі за допомогою електронних повідомлень і документів, що мають бути вчинені в електронному вигляді, або просто, щоб дозволити укладання договору, що має бути підтверджено за допомогою електронних засобів. Аналогічним чином, положення про електронний підпис в нормативно-правовій базі для електронної комерції дозволяють електронне виконання вимог про підписи, які можна застосувати до укладання договорів.

38. Нормативно-правові бази для електронної комерції (окрім підтримки електронного укладання договорів, що дозволяють обмін оферти і акцепту в електронній формі, а також дозволяють підписання за допомогою електронних еквівалентів) можуть містити ряд додаткових положень, які підтримують укладання договорів, і які наведено нижче.

39. Що стосується міжнародного уніфікованого договірного права в галузі договорів купівлі-продажу, в тому числі укладених в кіберпросторі, ключовим документом є Конвенція Організації Об'єднаних Націй про договори міжнародної

[33] Директива ЄС про електронну комерцію, стаття 9.2.

купівлі-продажу товарів, учасниками якої на момент написання цього документу є 85 країн, в тому числі Україна.[34] Ця Конвенція встановлює єдині міжнародні правила, що стосуються основоположних принципів укладання та виконання міжнародних договорів купівлі-продажу товарів. Слід зазначити, що одним з основоположних принципів цієї Конвенції є дотримання договірної свободи сторін домовлятися про свої права та обов'язки за договором.

Вимоги щодо форми

40. Конвенція ООН не накладає жодних конкретних вимог щодо форми повідомлення чи договору.[35] Такий підхід до договорів відповідає гнучкому підходу, прийнятому у багатьох країнах. У більшості країн-членів ЄС національне законодавство є досить гнучким і тенденція полягає в тому, щоб не застосовувати будь-які конкретної вимоги щодо форми при укладанні договору. Результатом цього є те, що письмовий документ не вимагається в якості чинного договору. Проте, підписаний документ у письмовій формі може відігравати певну роль в якості доказу того, що договір дійсно був укладений.

«Битва форм»

41. Проблема розбіжностей між умовами оферти та умовами акцепту («битва форм») може виникати у сфері електронної комерції так само, як вона виникає в традиційних паперових договорах. Залежно від застосовуваного договірного права, традиційні рішення можуть застосовуватися таким чином, що електронне акцептування, яке включає в себе суттєві розбіжності з офертою, було б рівнозначним відмові від оферти і контроферту. Електронний акцепт, який містив лише незначні відхилення від оферти, які істотно не змінюють оферту, може привести до укладення договору, який відображає ці незначні відхилення.

Можливість виправлення помилок

42. Ключовим засобом захисту прав споживачів в нормативно-правових документах у сфері електронної комерції є вимога, щоб покупцю було надано можливість виправити помилки, допущені при введенні інформації в електронні замовлення до остаточного розміщення замовлення.[36] Стандартна практика є такою, що якщо можливість виправити помилки не надається покупцеві, покупець повинен мати право відкликати ту частину електронного повідомлення, в якій була допущена помилка при введенні інформації (за умови, що покупець своєчасно

[34] http://www.uncitral.org/uncitral/en/uncitral_texts/sale_goods/1980CISG.html.
[35] UNCEC, стаття 9.1.
[36] Див. Директиву ЄС про електронну комерцію, стаття 11.1.

повідомив про помилку іншу сторону і не отримав матеріальної вигоди або вартості від іншої сторони).[37]

Використання автоматизованих систем повідомлень для укладання договору

43. Згідно з практикою укладання контрактів в контексті електронної комерції, правові рамки для електронної комерції поширюють принцип недискримінації на договори, укладені в результаті взаємодії автоматизованої системи повідомлень і фізичної особи, або шляхом взаємодії автоматизованих систем повідомлень.[38]

Розкриття інформації

44. Положення, що регулюють комерційні повідомлення в сфері електронної комерції, можуть включати в себе вимоги щодо розкриття інформації, пов'язаної з укладанням договору, принаймні, коли одержувачами комерційних повідомлень є споживачі (інформація, включаючи кроки, що призвели до укладання договору, умови договору, можливість для споживача виправити помилки в замовленні до його фактичного розміщення).[39]

Включення шляхом посилання

45. Положення даного типу дозволяють не обов'язково повністю включати умови договору в повідомлення даних, якими обмінюються сторони договору. Натомість вони можуть бути доступними шляхом посилання (наприклад, гіперпосилання) в повідомленні даних.[40]

Електронні ліцензійні угоди

46. Термін «електронна ліцензійна угода» (click-wrap agreement або click-to-accept agreement) описує ситуацію, коли будь-яка сторона погоджується з умовами для завантаження програмного забезпечення або купівлі товарів або послуг в режимі онлайн, натиснувши кнопкою опцію «Я погоджуюсь»» або «Я приймаю», яка з'являється в діалоговому вікні до виконання транзакції.

---

[37] UNCEC, стаття 14.1.
[38] UNCEC, стаття 12.
[39] Див., наприклад, Директиву ЄС про електронну комерцію, стаття 10.
[40] MLEC, стаття 5.

47. Термін «електронна ліцензійна угода» (click-wrap agreement) походить від терміну «упакована ліцензійна угода» (shrink-wrap agreement), який стосується практики забезпечення виконання ліцензійних угод на програмне забезпечення, які набувають чинності після розкриття користувачем упаковки, що містить копію умов ліцензійної угоди. Як у випадку електронної ліцензійної угоди, так і у випадку упакованої ліцензійної угоди від покупця вимагаються фізичні дії, щоб погодитись з умовами ліцензійної угоди.

48. Поняття «електронна ліцензійна угода» може відрізнятися від того, що іноді називають «browsewrap угодою", яка може передбачати менше активних дій з боку користувача і означає лише пасивну поведінку користувача, наприклад, використання веб-сайту або вихід за межі домашньої сторінки веб-сайту, без необхідності надання будь-якого або досить чіткого і помітного повідомлення про будь-які умови.[41]

I. Постачальники проміжних послуг

Вимоги щодо розкриття інформації

49. Положення нормативно-правової бази для електронної комерції, що стосуються діяльності постачальників проміжних послуг (ППП) можуть включати в себе вимоги щодо розкриття інформації одержувачам про ППП (наприклад, ім'я, адреса і контактна інформація ППП). Додаткові вимоги до розкриття інформації можуть застосовуватися в разі комерційних повідомлень (зокрема, повідомлення, призначені для реклами та продажу товарів і послуг). Наприклад, можуть знадобитися рекламні пропозиції, які включають в себе інформацію про умови, які повинні бути виконані, щоб скористатися ними.[42]

Режим відповідальності для постачальників проміжних послуг

50. Одним з ключових питань, що розглядаються в нормативно-правовій базі для електронної комерції, є питання про відповідальності постачальників проміжних послуг (ППП), коли вони займаються лише передачею або зберіганням інформації або лише хостингом.

---

[41] Для подальшого обговорення цих питань, див. "The Clicks That Bind: Ways Users "Agree" to Online Terms of Service", блогпост Еда Бейлі на сайті Electronic Frontier Foundation (листопад 2009 р.) https://www.eff.org/wp/clicks-bind-ways-users-agree-online-terms-service.

[42] Приклади таких положень можна знайти в Директиві ЄС про електронну комерцію, стаття 5 (стосовно загальної інформації) та стаття 6 (у разі комерційних повідомлень).

51. Загальний підхід полягає в тому, що, обмежуючись участю лише у таких пасивних видах діяльності, ППП має право на звільнення від відповідальності за порушення, в тому числі можливі протиправні дії тих, хто користується їхніми послугами. Наприклад, Директива ЄС про електронну комерцію передбачає звільнення від відповідальності лише за «передачу інформації» і «кешування» (зберігання інформації), право на яке ППП має, за умови, якщо він жодним чином не займається змістом інформації, що завантажується, передається або зберігається, не змінює інформацію, та обізнаний із фактами чи обставинами, з яких випливає незаконна діяльність, та не бере участі у будь-якій незаконній діяльності.[43]

52. Як тільки ППП почне відігравати більш активну роль, наприклад, почне свідомо співпрацювати з одержувачем своїх послуг у здійсненні незаконної діяльності, він втрачає право на звільнення від відповідальності. Проте, якщо не брати до уваги тих постачальників послуг, які беруть участь в незаконній діяльності, ППП набуває зобов'язання втрутитися, щоб не допустити незаконну діяльність або вилучити порушуючі матеріали після того, як йому стане відомо про незаконну діяльність, або після того, як йому буде наказано це зробити компетентним судом або адміністративним органом.
Такі випадки звільнення від відповідальності підтримуються нормою про те, що ППП, як правило, не зобов'язані контролювати дії користувачів їх послуг. Водночас, такі види привілеїв не виключають можливості законодавчого закріплення обов'язку ППП вживати необхідний ступінь заходів безпеки.[44]

J. Застосовність по відношенню до державних органів

53. Практика регулювання різних держав відрізняється в залежності від того, яким чином і в яких масштабах деякі основні методи електронної комерції, що стосуються інформації в електронній формі, приймаються для урядових/адміністративних цілей. Це питання стосується повідомлень і обміну даними між державними структурами, а також між урядом і громадянами (G2P) та між урядом і бізнесом (G2B).

54. У деяких країнах застосовується дозвільний підхід, що дає державним органам можливість самим вирішувати, якою мірою приймати повідомлення та документи від громадян і компаній, а також здійснювати обмін документами та інформацією в електронному вигляді на урядовому рівні. У деяких країнах застосовуються схожі підходи, які можуть включати регламентування практик, технічних стандартів та протоколів, які повинні застосовуватися. Це може охоплювати й підтвердження загальної норми про те, що електронні документи та

[43] Директива ЄС про електронну комерцію, статті 12-15 та параграфи 40-48 декларативної частини цієї Директиви.
[44] Директива ЄС про електронну комерцію, параграф 48 декларативної частини.

матеріали вважаються ефективними для цілей виконання вимог закону щодо письмових документів, в тому числі, для адміністративних цілей.

55. Таким чином, в одних випадках виявляється, що чинне законодавство фактично не вимагає від державних адміністративних органів приймати електронні повідомлення та документи, тоді як в інших випадках законодавство заходить настільки далеко, що зобов'язує органи державного управління приймати електронні документи під час обміну інформацією з громадянами та бізнесом, а також при обміні інформацією і документами між державними органами.

56. Питання, які можуть бути розглянуті при регулюванні документообігу та обміну даними між державними органами, включають в себе:

(a) впровадження єдиних правил для всіх урядових структур щодо обміну даними, файлами, інформацією в різних реєстрах;
(b) взаємодія інформаційних систем;
(c) відповідальність за перевірку точності та юридичної сили інформації та її оновлення;
(d) електронне архівування документів державними органами та взаємодія з центральними державними архівами;
(e) уніфікація інформації, що зберігається в двох примірниках в різних місцях.

57. Якщо прийом електронних повідомлень або документів залишається гнучким або застосовується вибірково, при прийнятті рішення можуть мати значення різні фактори. До їх числа відносяться: тип адміністративних процедур або відповідних транзакцій; наявність технічної інфраструктури (наприклад, для електронних підписів); та норми чинного законодавства і нормативні акти, в тому числі правила та правові документи, що стосуються електронного уряду.

58. Громадянам та компаніям, що здійснюють обмін інформацією з державними органами, як правило, надається вибір – використовувати електронні або інші традиційні засоби зв'язку – хоча компанії, більш ймовірно, зіткнуться, принаймні, з деякими вимогами щодо електронного обліку (наприклад, для цілей оподаткування).

59. Прийом і використання державними органами електронних документів або їх відсутність можуть мати наслідки для ефективності діяльності приватного сектора і ступеня запровадження приватним сектором електронних процедур у своїй діяльності. Неприйняття електронних документів державними органами може бути стримуючим фактором для запровадження, наприклад, електронного інвойсування компаніями, тим самим підкреслюючи тісний зв'язок між електронним урядом і законодавством та ініціативами у сфері електронної комерції.

Частина II. Додаткові питання, що стосуються нормативно-правової бази електронної комерції

A. Оборотні документи

60. Однією з найбільш складних областей розробки нормативно-правової бази для електронної комерції є обігові інструменти, такі як переказні векселі (прості векселі) та транспортні накладні (транспортні документи, як правило, на морському транспорті). Такі оборотні (обігові) документи наділяють їх власників певними правами:

- у разі переказних векселів, такий інструмент уособлює право його власника отримати зазначену в ньому суму, та
- у разі транспортної накладної, такий інструмент втілює в собі не тільки договір перевезення, але також право його власника на отримання товару і право власності на нього.

61. Основною причиною труднощів застосування таких інструментів у сфері електронної комерції є той факт, що ці інструменти самі по собі уособлюють особливе право їх власника на отримання певної виплати, або, у разі транспортної накладної, такий інструмент втілює в собі право власності на відповідний товар.

62. Така роль цих типів інструментів головним чином пояснюється тим, що існує один, унікальний документ (не дубльований), що втілює право власника єдиного, унікального документа на отримання виплати або, у разі транспортної накладної, набути право власності на товар. Оборотність векселя або транспортної накладної (тобто можливість передавати або продавати ці інструменти) була заснована на наявності унікального документа в кожному окремому випадку, яким одночасно міг володіти тільки один власник.

63. Отже, в електронному контексті, проблема полягала в тому, як відтворити і захистити цю унікальність (сингулярність) переказного векселя або транспортної накладної, що відображає елемент володіння інструментом його власником, і, в той же час, надає можливість його передачі іншій особі (наприклад, покупець, якому належить транспортна накладна, може продати товар під час його переміщення (новому покупцеві, який стане новим власником транспортної накладної і матиме право прийняти товар або продати його новому індосату)).

64. Є кілька прикладів спроб відтворити ці характеристики обігового документа в електронному середовищі за допомогою електронних функціональних еквівалентів, зокрема, в транспортному секторі. Основним прикладом таких зусиль може служити Конвенція Організації Об'єднаних Націй про договори міжнародного перевезення вантажу повністю або частково морем (2009 р.), відома як «Роттердамські правила»). Окрім того, що Роттердамські правила містять різні положення, які дозволяють використовувати електронні функціональні еквіваленти для виконання різних формальних вимог (наприклад, вимоги щодо письмової форми), вони дозволяють таке використання електронних функціональних еквівалентів транспортних документів, у тому числі обігових електронних транспортних накладних («електронний обіговий транспортний запис»).

65. Відповідні положення Роттердамських правил покликані встановити електронні функціональні еквіваленти ключових характеристик електронного обігового транспортного документа, тобто

- унікальність (сингулярність) документа (існування лише в одному екземплярі),
- його приналежність власнику, та
- можливість передачі документа іншій особі (що дозволяє продати відповідний товар під час його транспортування).

66. Стаття 9 Роттердамських правил встановлює процедурні вимоги, які повинні бути виконані (і які зазначені в договорі між вантажовідправником і перевізником) для електронного обігового транспортного документа, що буде використовуватися:

> «І. Використання обігового електронного транспортного запису здійснюється у відповідності з процедурами, які передбачають:
> (a) метод видачі та передачі цього запису передбачуваному власнику;
> (b) підтвердження збереження цілісності обігового електронного транспортного запису;
> (c) спосіб, в який власник може продемонструвати, що він є таким власником; та
> (d) спосіб надання підтвердження того, що здача вантажу власнику була здійснена або що відповідно до пункту 2 статті 10 або підпунктів (a) (ii) та (c) пункту 1 статті 47 електронний транспортний запис повністю втратив юридичну силу або чинність».

67. Додаткові допоміжні положення Роттердамських правил включають в себе, зокрема:

> *В статті 47 (Здача вантажу в тому випадку, коли обіговий транспортний документ або електронний обіговий транспортний запис видані)*

зазначається:

«І. Якщо обіговий транспортний документ або обіговий електронний транспортний запис видані:

(a) власник обігового транспортного документа або обігового електронного транспортного запису має право вимагати від перевізника здачі вантажу після його прибуття в місце призначення…».

У статті 51 (Ідентифікація контролюючої сторони і передача права контролю над вантажем) зазначається:

« …

4. Якщо виданий обіговий електронний транспортний запис:
(a) власник є контролюючою стороною;
(b) власник може передати право контролю над вантажем іншій особі шляхом передачі обігового електронного транспортного запису у відповідності з процедурами, зазначеними в пункті 1 статті 9; та
(c) для здійснення права контролю над вантажем власник повинен довести, у відповідності з процедурами, зазначеними в пункті 1 статті 9, що він є власником».

У статті 57([передача прав] Випадки, коли обіговий транспортний документ або обіговий електронний транспортний запис видані) зазначається:

«…
2. Якщо виданий обіговий електронний транспортний запис, його власник може передати права, закріплені в цьому електронному транспортному записі, незалежно від того, чи був він виданий за розпорядженням поіменованої особи, шляхом передачі електронного транспортного запису у відповідності з процедурами, зазначеними в пункті 1 статті 9».

68. Слід зазначити, що Комісія Організації Об'єднаних Націй з права міжнародної торгівлі (ЮНСІТРАЛ), яка була органом Генеральної Асамблеї ООН, який розробив Роттердамські правила, в даний час розробляє шаблон, який країни можуть використовувати при розробці законодавчих положень, що підтримують використання електронних обігових інструментів (проект Типового закону про електронні обігові записи).

69. Поточна версія проекту Типового закону містить ряд положень, спрямованих на визначення ключових елементів обіговості в електронному середовищі. Щоб проілюструвати такий підхід, наступне положення встановлює

основні елементи поняття «контролю» власника електронного обігового запису, що забезпечує електронний функціональний еквівалент традиційного, паперового поняття володіння власником обігового інструменту:

«**Проект статті 10. Контроль**

1. Якщо закон вимагає володіння обіговим документом або інструментом, ця вимога вважається виконаною щодо електронного обігового запису, якщо використовується надійний метод:

(a) для встановлення виняткового контролю над цим електронним обіговим записом будь-якої особи; та
(b) для визначення цієї особи як особи, яка здійснює контроль.

2. Якщо закон вимагає чи дозволяє передачу володіння обіговим документом або інструментом, це вимога задовольняється щодо електронного обігового запису шляхом передачі контролю над електронним обіговим записом».

B. Мобільні гроші

Основи

70. «Мобільні гроші» (також відомі як «м-гроші»), які використовуються в широкому сенсі, передбачають використання мобільних портативних пристроїв для платіжних та інших фінансових послуг (наприклад, інтерактивний доступ до банківських рахунків, мобільні платіжні послуги з використанням небанківських установ, таких як оператори мобільних мереж зв'язку, зберігання мобільних грошей в мобільних портативних пристроях).

71. Мобільні гроші є частиною більш широкої сфери розвитку електронної комерції, яка відома як «м-комерція» (тобто «мобільна комерція», яка використовує невеликі портативні пристрої, в тому числі мобільні телефони, планшети тощо, які зазвичай мають можливість здійснювати обмін повідомленнями та доступ до інтернету).

72. «е-гроші» є «передоплаченим» інструментом або продуктом, «який

(i) видається при отриманні грошових коштів,
(ii) включає записану в електронному вигляді грошову суму, яка зберігається на пристрої (тобто, в

комп'ютерній системі, мобільному телефоні, карті передоплати або чіпі),

(iii) приймається як засіб платежу іншими сторонами, ніж емітент, та

(iv) може бути конвертований в готівку»[45]

73. Мобільні гроші характеризуються як різновид електронних грошей, оскільки вони відносяться до «фінансових послуг та транзакцій, що здійснюються за допомогою мобільного телефону»[46].

74. Переваги, які забезпечують мобільні гроші, включають в себе той факт, що вони передбачають використання інтерактивних пристроїв в автономному режимі (на відміну від платіжних карт, які вимагають додаткового пристрою для того, щоб бути інтерактивними, наприклад, для перевірки залишків коштів на рахунках), мобільні гроші знаходяться в мобільному телефоні, який також є засобом зв'язку (на відміну від платіжної карти), до того ж мобільні телефони мають властивість забезпечувати платежі в дистанційному режимі (на відміну від платіжних карт, які вимагають додаткового пристрою або наявності Інтернету чи телефону)[47].

75. М-гроші слугують важливим інструментом для фінансового включення (тобто для надання доступу до фінансових послуг тим, хто традиційно зовсім не отримував таких послуг або отримував їх в недостатній мірі) і отже, можуть стати важливим двигуном розвитку і засобом боротьби з бідністю. Крім того, м-гроші є зручним інструментом. Наприклад, м-гроші пов'язані з можливістю використовувати мобільний пристрій для платежів з використанням технології ближнього безконтактного зв'язку. Це дозволяє використовувати мобільні пристрої для здійснення оплати через касові термінали шляхом піднесення пристрою до зчитувача ближнього безконтактного зв'язку в місці продажу або оплати (наприклад, для оплати за паркування в підземному паркінгу).

Бізнес-моделі, що використовують м-гроші

76. На практиці були розроблені різні базові прототипи, в тому числі

- керовані операторами мобільних мереж зв'язку,
- керовані банками, та
- змішаного типу (між операторами мобільних мереж зв'язку та банками)

[45] Supervising Nonbank E-Money Issuers, CGAP Brief, липень 2012 р., http://www.cgap.org/sites/default/files/CGAP-Brief-Supervising-Nonbank-Emoney-Issuers-Jul-2012.pdf

[46] Див. Звіт Міжнародної фінансової корпорації, IFC Mobile Money Study 2011 Summary Report, стор. 2.http://www.ifc.org/wps/wcm/connect/industry_ext_content/ifc_external_corporate_site/industries/financial+markets/publications/mobile+money+study+2011

[47] Там же, стор. 14.

- створення незалежного оператора мобільних грошей, який працює з операторами мобільних мереж зв'язку і, можливо, також з банками, які створюють пов'язані рахунки, та
- встановлення оператором мобільних грошей партнерських відносин з рітейлерами для оплати рахунків.[48]

77. Оператори мобільних мереж зв'язку можуть мати найбільший стимул для виходу на ринок м-грошей, зокрема, тому, що вони володіють мережевою інфраструктурою та клієнтською базою абонентів.

Користувачі м-грошей

Фінансові послуги

78. Основні види використання м-грошей включають в себе перекази грошових коштів і, в залежності від типів доступних послуг, платежі (які можуть бути дистанційними або з використанням технології ближнього безконтактного зв'язку). Можливі додаткові фінансові послуги включають в себе заощадження, кредити і страхування (наприклад, для страхових виплат). Надання таких додаткових фінансових послуг може передбачати наявність зв'язку між оператором мобільних мереж зв'язку і банком (див, наприклад, M-Kesho в Кенії[49]).

Використання ефірного часу в якості валюти

79. Ще однією можливістю є використання мобільного ефірного часу в якості валюти для купівлі товарів і послуг. Незважаючи на те, що вона виникла дещо несподівано, використання невитраченого мобільного ефірного часу в якості валюти, а також в якості ходового товару, є явищем, яке набуває дедалі більшого поширення на міжнародному рівні. Різні оператори пропонують продаж ефірного

[48] Див. Keith Donovan, "Mobile Money for Financial Inclusion", Chapter 4 in World Bank, Information and Communications for Development: Maximizing Mobile (2012), стор. 67. (http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/IC4D-2012-Report.pdf).

[49] M-Kesho передбачає наявність зв'язку між Safaricom, кенійським мобільним оператором, який використовує систему M-PESA, і Equity Bank, для відкриття відсоткового мікроощадного рахунку. Абонент може переказувати кошти з рахунку M-KESHO абонента в Equity Bank на рахунок M-PESA абонента, а також робити перекази з рахунку M-PESA на рахунок M-KESHO. Інші особливості цього рахунку включають надання мікрокредитів (екстрений кредит, який надається через M-PESA), мікрострахування, а також особисте страхове покриття від нещасного випадку, яке можна отримати в повному обсязі через 1 рік. Для того, щоб відкрити цей рахунок, потрібно бути абонентом M-PESA. http://www.safaricom.co.ke/personal/m-pesa/m-pesa-services-tariffs/m-kesho.

часу в різних країнах. Такі міжнародні перекази, за деякими оцінками, зросли вдвічі – з $ 350 млн до $ 700 млн у 2012 році[50].

80. Оскільки використання ефірного часу в якості валюти може призвести до зростання побоювань з приводу підозрілої діяльності, можуть бути запроваджені відповідні запобіжні заходи, такі як встановлення лімітів на перекази та збирання інформації про покупців і продавців ефірного часу, а також інші заходи подібного типу, зазначені в рекомендаціях Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF)[51].

Використання м-грошей урядом

81. Використання урядом м-грошей для платежів (зокрема, для виплати урядом заробітної плати та пенсій фізичним особам (G2P)) може стимулювати зростання м-грошей в економіці в цілому.[52] Воно також може принести важливу користь у вигляді зниження корупції. G2P платежі також сприяють досягненню цілі політики розширення доступу населення до фінансових послуг.[53] Якщо на платіжну систему G2P для конкретної урядової програми соціальних виплат оголошується тендер, уряд може зажадати від учасників тендеру, щоб вони запропонували здійснення оплати за допомогою таких методів, як м-гроші, які сприяють розширенню доступу до фінансових послуг, а також може включити вимогу про надання додаткових фінансових послуг користувачам платіжної системи G2P (наприклад, ощадні рахунки).[54]

Міжнародні грошові перекази

82. Міжнародне використання м-грошей може сприяти зменшенню транзакційної вартості грошових переказів. Незалежно від того, чи використовуються м-гроші або інші форми і механізми електронних грошей,

[50] "Airtime is money – The use of pre-paid mobile-phone minutes as a currency", Economist, 15 січня 2013 р., http://www.economist.com/news/finance-and-economics/21569744-use-pre-paid-mobile-phone-minutes-currency-airtime-money.

[51] Група з розробки фінансових заходів боротьби з відмиванням грошей, Guidance for a Risk-Based Approach – Prepaid Cards, Mobile Payments and Internet-Based Payment Services (http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf).

[52] McKinsey (для Bill and Melinda Gates Foundation), Inclusive Growth and Financial Security: The benefits of e-payments to Indian society (2010), стор. 7, доступно на http://mckinseyonsociety.com/inclusive-growth-and-financial-security/.

[53] Консультативна група з надання допомоги найбіднішим верствам населення (CGAP) та DIFID, Banking the Poor via G2P Payments, http://www.cgap.org/sites/default/files/CGAP-Focus-Note-Banking-the-Poor-via-G2P-Payments-Dec-2009.pdf «Оскільки уряди все частіше переходять на надання послуг через систему G2P в електронній формі, вони також створюють можливість надання фінансових послуг тим же самим одержувачам».

[54] Там же, стор. 16; деякі питання організації тендера на систему платіжного сервісу G2P з метою спробувати забезпечити досягнення цілей ефективності, а також розширення доступу населення до фінансових послуг (дистанційний банкінг) викладені на стор. 18.

міжнародні грошові перекази є тим напрямком, в якому спостерігається значне зростання і активність. Одне нещодавнє дослідження показало, що використання м-горошей веде до зниження вартості міжнародних грошових переказів (в середньому більш ніж на 50 відсотків дешевше в порівнянні з вартістю відправки грошей) за рахунок посилення конкуренції, використання існуючих мереж та інфраструктури, а також віднімання все більшої частки ринку дешевших транзакцій від традиційних глобальних операторів грошових переказів.[55] Таким чином, використання м-грошей для міжнародних грошових переказів безпосередньо сприяє досягненню Цілі сталого розвитку 10с ООН (скорочення витрат емігрантів на переказ грошових коштів), а відтак розширенню доступу до фінансових послуг та інших цілей розвитку.

83. Різні типи моделей міжнародних грошових переказів впроваджуються на практиці, а також допомагають знизити витрати споживачів. До їх числа належать міжнародні грошові перекази через систему mWallets, використання онлайн-платформ для відправки переказів, альтернативи моделям на мобільній основі і таким, що передбачають переведення в готівку, які дозволяють відправнику обмежити сферу використання грошових переказів (наприклад, подарункові кредитні картки для конкретного комерсанта або постачальника послуг, або безпосередня оплата рахунків одержувача), онлайн-перекази з використанням соціальних медіа, альянси за участю операторів мобільного зв'язку, які працюють в партнерстві, або спільно з операторами грошових переказів, такими як Western Union і MoneyGram, з глобальними хабами у сфері грошових переказів, а також з фінансово-технологічними компаніями (останні дозволяють прямі грошові перекази з одного телефону на інший без участі агентів з прийому та видачі готівки). Можна очікувати, що по мірі розширення використання і функціональних можливості м-грошей, міжнародні грошові перекази з використанням м-грошей та інші еманації електронних грошей буде продовжувати рости.[56]

84. Проте існує потенціал для значного зростання. Хоча у звіті за 2015 рік було виявлено, що міжнародні грошові перекази є найбільш швидко зростаючою послугою з використанням м-грошей і зросли на 52 відсотки в порівнянні з попереднім роком, міжнародні грошові перекази все ще можуть здійснюватись

[55] Міжнародна асоціація GSM (GSMA), Driving a price revolution: Mobile money in international remittances (жовтень 2016 р.), стор. 5 (http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/10/2016_GSMA_Driving-a-price-revolution-Mobile-money-in-international-remittances.pdf); Додаткову інформацію про нові моделі партнерства можна знайти на стор. 9 останнього звіту GSMA.

[56] Стосовно подій в галузі міжнародних грошових переказів, див. Wameek Noor and Andria Thomas, International Remittances and Branchless Banking: Emerging Models, 18 липня 2013 р. http://www.cgap.org/blog/international-remittances-and-branchless-banking-emerging-models; результати детального дослідження змін в сфері міжнародних грошових переказів за 2013 рік представлені в http://www.slideshare.net/CGAP/international-remittances-through-branchless-banking.

безпосередньо з мобільних телефонів лише в 16 з 93 країн, де надаються послуги з використанням мобільних грошей.[57]

85. Із зростанням міжнародних грошових переказів, а також поширенням компаній у сфері грошових переказів в різних місцях і юрисдикціях може виникнути необхідність у вирішенні регуляторних питань за рахунок розширення масштабів спільного використання центральними даних про клієнтів на міжнародній основі центральними банками, регулюючими та правоохоронними органами.[58]

Функціональна сумісність

86. Функціональна сумісність є ключовим стимулюючим фактором при розробці та впровадженні м-грошей. Функціональна сумісність означає здатність мобільної платіжної системи взаємодіяти з операторами систем платіжних та фінансових послуг на різних рівнях і в різних можливих ступенях. Функціональна сумісність визначає, чи обмежуються рамки послуг з грошових переказів клієнтами одного оператора мобільного зв'язку, або клієнти різних операторів мобільного зв'язку можуть переказувати м-гроші один одному (тобто без урахування того, SIM-карта якої компанії знаходиться в телефоні), забезпечуючи тим самим можливість загального визнання (як при передачі текстових повідомлень між різними платформами).

87. Ще одним аспектом взаємодії є необхідність бути в змозі досягти користувачів мобільних телефонів будь-якого типу, тобто не лише тих, що мають смартфони (з доступом до Інтернету), а й тих, що користуються тільки простими мобільними телефонами.

88. Хоча багато хто вважає це питанням віддаленого майбутнього, в напрямку взаємодії між операторами мобільного зв'язку вже досягнуто значного прогресу. Питання, пов'язані з функціональною сумісністю на рівні платформ, [59] включають в себе можливість доступу через банкомати, касові термінали в точках продажу, а також доступ через агентів і взаємодію агентів.

Ризики та заходи безпеки

[57] GSMA, 2015 State of the Industry Report: Mobile Money, стор. 7. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/04/SOTIR_2015.pdf, and GSMA, Driving a price revolution: Mobile money in international remittances, вище, зноска 56, стор. 15.
[58] Це було рекомендацією дослідження, підготовленого в Сполучених Штатах для Федерального резервного банку Атланти Синтією Мерріт, Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments, Retail Payments Risk Forum White Paper (серпень 2010), http://www.frbatlanta.org/documents/rprf/rprf_resources/wp_0810.pdf.
[59] Platform-level Interconnection in Branchless Banking (18 січня 2012 р.), http://www.cgap.org/blog/platform-level-interconnection-branchless-banking.

89. Основні ризики при випуску м-грошей, так само, як у випадку електронних грошей в цілому, як правило, включають в себе:

(a) недостатність коштів, виділених в надійних, ліквідних інвестиціях для задоволення попиту клієнтів на готівкові кошти;
(b) недостатність коштів для виплати клієнтам у разі банкрутства емітента (або довіреної особи/фідуціарія);
(c) недостатність активів для виплати клієнтам у разі банкрутства банку;
(d) кримінальна діяльність (наприклад, відмивання грошей).

90. З точки зору розвитку електронної комерції, бажано, щоб регуляторне середовище не перешкоджало розвитку м-грошей і водночас забезпечувало адекватне вирішення проблем регуляторного характеру. Таким чином, фундаментальне питання політики, яке необхідно розглянути, стосується ступеня регуляторного обтяження, яке має бути накладено на розвиток і функціонування ринку мобільних фінансових послуг.

91. Регулятивний підхід, який застосовується щодо м-грошей, особливо на ранній стадії розвитку, включаючи ступінь відкритості для нових учасників (наприклад, небанківських суб'єктів, таких як оператори мобільного зв'язку) і інновації, а також ступінь впевненості і передбачуваності, є важливими аспектами, які, в залежності від того, як вони відкалібровані, можуть визначати успіх або його відсутність при запровадженні м-грошей.[60] Серед інших регуляторних питань, які можуть виникнути, спектр фінансових послуг, які може запропонувати випуск м-грошей, якщо це небанківська установа.

Заходи захисту від ризику втрати або відсутності коштів [61]

92. Такі захисні заходи включають[62]:

[60] Згідно зі звітом Міжнародної фінансової корпорації IFC Summary Report, вище, зноска 47, стор. 35, «як і очікувалось, регуляторне середовище є вирішальним параметром, який може або створити, або не допустити можливість для бізнесу, пов'язаного з мобільними грошима». Схожі аспекти відкритості та визначеності в регуляторному середовищі на ранніх етапах розвитку нового ринку приписують Девіду Портеосу, The Enabling Environment for Mobile Banking in Africa (2006, звіт, підготовлений DIFID), стор. 14 (http://www.microfinancegateway.org/gm/document-1.9.25001/36204_file_M_banking_Enab_Env.pdf).

[61] Огляд можливих заходів для забезпечення захисту грошей клієнтів наведений у Mobile Money: Enabling regulatory solutions, посібнику GSMA, підготовленому С. Ді Кастрі (лютий 2013 р.), стор. 15-18, доступний на http://www.gsma.com/publicpolicy/wp-content/uploads/2013/02/GSMA2013_Report_Mobile-Money-EnablingRegulatorySolutions.pdf; також див. Safeguarding Mobile Money: How providers and regulators can ensure that customer funds are protected, посібник GSMA (січень 2016 р.), http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/01/2016_GSMA_Safeguarding-Mobile-Money_How-providers-and-regulators-can-ensure-that-customer-funds-are-protected.pdf.

(a) *Ліквідність* – ключовим принципом, що застосовується для збереження коштів, є ліквідність - активи повинні бути ліквідними та необтяженими, щоб забезпечити наявність необхідних коштів для переведення коштів клієнта в готівку.

(b) *Необхідні резервні депозити* – вимога до небанківських емітентів тримати на депозиті в установі, що перебуває під розсудливим наглядом (наприклад, банк), або в авторизованій ліквідній інвестиції (наприклад, державні цінні папери) грошову суму, еквівалентну загальній сумі випущених електронних грошей (або мобільних грошей) (цю суму іноді називають на практиці «електронна касова готівка»).

(c) *Відокремлення коштів клієнтів* – кошти клієнтів, як правило, повинні триматися на окремому або виділеному рахунку, окремо від інших коштів небанківського емітента, і, таким чином, мають бути захищені від кредиторів небанківського емітента. У деяких системах це робиться за допомогою передбачених законом методів, таких як трастовий рахунок.

(d) *Страхування депозитів* – зберігання небанківськими емітентами депозитів, пов'язаних з випуском електронних грошей, піднімає питання про можливість застосування страхування депозитів по відношенню до рахунків небанківських емітентів, на яких зберігаються кошти клієнтів. Як правило, такі схеми страхування пов'язані з діяльністю у сфері прийняття депозитів, з якої введення в обіг електронних грошей, як правило, було виключено. Існує також той факт, що сума грошей на депозиті перевищує сумму страхового покриття відповідного депозиту. Існує прецедент для цього, зокрема, якщо таке страхування спрямоване на суми залишків на рахунку окремого клієнта[63].

(e) *Обмеження на використання коштів емітентом* – це може включати в себе обмеження, згідно з яким кошти можуть використовуватись тільки для погашення фінансових зобов'язань перед клієнтами (повернення коштів клієнтам, а також для здійснення платежів торговцям за дорученням клієнта), а не для покриття операційних витрат, пов'язаних з випуском, або для будь-яких інших цілей; вкладення захисних коштів на депозит може бути обмежено деякими певними типами інструментів. Інше поширене обмеження полягає в тому, щоб не дозволяти емітентам електронних грошей використовувати гроші клієнтів для видачі кредитів (позик) (відсутність посередництва).

---

[62] Частково базується на публікації Майкла Тараці та Пола Брелоффа, CGAP Focus Note No. 63, Nonbank E-Money Issuers: Regulatory Approaches to Protecting Customer Funds, липень 2010 р., стор. 2 http://www.cgap.org/publications/nonbank-e-money-issuers.

[63] The CGPAP Brief, Supervising Nonbank E-Money Issuers, вище, зноска 46, стор. 8, наводить приклад Сполучених Штатів, кошти, пов'язані з картками для поповнення рахунку, вважаються депозитами для цілей схеми страхування депозитів за умови, що такі кошти зберігаються на депозиті в установі згідно зі схемою страхування депозитів. Альтернативним підходом, який розглядається в цьому документі, є збільшення ліміту страхування для об'єднаних рахунків.

Заходи захисту від ризику незаконної діяльності

93. Занепокоєння, яке наводиться в якості аргумента на підтримку прийняття більш обмежувальної політики щодо розвитку м-грошей, пов'язано з боротьбою з відмиванням грошей і фінансуванням тероризму і правовими міркуваннями. Проте одним із сильних контраргументів є те, що м-гроші насправді можуть сприяти збільшенню прозорості фінансових переказів і підвищенню здатності контролюючих і правоохоронних органів відстежувати рух грошових коштів, збирати податки та іншим чином боротися з незаконною діяльністю. М-гроші виводять значний обсяг грошових переказів з тіні, що дозволяє їх облік, контроль і аудит з боку органів влади, тоді як раніше вони здійснювались на строго касовій основі без контролю чи аудиту.[64]

94. У будь-якому разі, засоби захисту м-грошей, які можуть зменшити ризик незаконної діяльності, а також забезпечити проведення розслідування та примусове виконання, включають в себе встановлення лімітів по транзакціях, застосування процедури ідентифікації «знай свого клієнта» (ЗСК), а також вимог до обліку і звітності.

Вимоги «знай свого клієнта»

95. Одним з основних засобів захисту від незаконної діяльності є ідентифікація клієнта (належна перевірка клієнта), яка зазвичай відома як вимоги «знай свого клієнта». При розробці вимог ЗСК може бути застосований принцип пропорційності відповідно до підходу, що передбачає пропорційне врахування факторів ризику.[65] Наприклад, в рамках багаторівневого підходу до вимог ЗСК, такі вимоги можуть бути мінімальними або незастосовними для рахунків нижчого рівня і більш жорсткими для рахунків більш викого рівня[66].

[64] Наприклад, у Звіті McKinsey за 2010 р., який згадується вище, зноска 53, робиться висновок про те, що однією із стратегічних переваг буде «зменшення відмивання грошей за рахунок більш широкого доступу до інформації про рух грошових коштів в країні» (стор. 13), http://gssp.newamerica.net/sites/gssp.newamerica.net/files/articles/inclusive%20growth%20and%20financial%20security.pdf.

[65] Див. International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations, Група з розробки фінансових заходів боротьби з відмиванням грошей (лютий 2012 р.), Рекомендація 1, стор. 11 http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

[66] Приклад такого багаторівневого підходу можна знайти в Циркулярі № 09 2011 року Департаменту банківськох політики Державного банку Пакистану, яким були внесені зміни до Положення про дистанційний банкінг 2008 року. Ці зміни включали в себе введення рахунку «нульового рівня», який являє собою рахунок мобільного гаманця з найнижчими лімітами на транзакції і який може бути відкритий в електронному вигляді без пред'явлення будь-яких паперових документів. (Див. Chris Bold, State Bank of Pakistan Removes Barriers to Branchless Banking, 25 липня 2011 р., http://www.cgap.org/blog/state-bank-pakistan-removes-barriers-branchless-banking; текст змін можна знайти за посиланням http://www.sbp.org.pk/bprd/2011/C9-Enclosure-1.pdf). Інші заходи щодо

Грошові обмеження

96. Одним з регуляторних методів, які зазвичай застосовуються до м-грошей, є введення грошових обмежень на використання м-грошей. Ці обмеження в основному існують у вигляді лімітів на транзакції (ліміти на грошову вартість транзакцій) і лімітів на залишки на рахунку (ліміти на суму м-грошей, яку власник рахунку може мати у будь-який момент часу, або відповідно до встановленої розбивки на окремі періоди часу). Крім інших ризиків, які можуть бути зменшені за допомогою грошових обмежень, вони також допомагають стримувати системний ризик, якщо може бути проблемою регуляторних органів.

97. Ліміти на транзакції можуть бути поділені на категорії, такі як денні ліміти, місячні ліміти та річні ліміти. Для того, щоб стимулювати більш широке застосування м-грошей або інших форм електронних грошей, окремі системи переглянули і збільшили або усунули деякі з таких обмежень[67]. Інші можливі варіанти обмежень на транзації можуть бути різними для м-грошей, випущених спільно оператором мобільного зв'язку і банком.[68]

Регуляторний підхід

Міркування та принципи

98. Фактори, що свідчать на користь того, щоб дозволити небанківським установам (зокрема, операторам мобільного зв'язку) стати емітентами м-грошей, а також полегшений ступінь контролю, включають в себе, наприклад, [69]:

(a) відносно обмежені масштаби діяльності небанківських емітентів електронних грошей і обмежений обсяг транзакцій, які вони обробляють;
(b) той факт, що небанківські емітенти, як правило, не несуть системного ризику через відносно невелику суму коштів, яка представлена діяльністю таких емітентів;

лібералізації ЗСК включали скасування необхідності реєстрації біометричних даних у вигляді відбитків пальців для відкриття рахунку, зберігаючи при цьому більш дешеві механізми створення цифрового зображення власника рахунку.

[67] Наприклад, у 2011 році Державний банк Пакистану збільшив ліміти по транзакціях і усунув ліміти на залишки на рахунку 1 рівня, щоб стимулювати більш широке впровадження дистанційного банківського обслуговування; для рахунків нижнього (нульового) рівня, застосовується максимальний ліміт залишку у розмірі 100000 пакистанських рупій (див. Циркуляр № 09 2011 року Департаменту банківської політики Державного банку Пакистану, вище, зноска 67, стор. 2).

[68] Так було у випадку з грошима Iko Pesa в Кенії, які були випущені оператором мобільного зв'язку Orange спільно з Equity Bank (див. IFC Summary Report, вище, зноска 47, стор. 9).

[69] Ці фактори згадуються, наприклад, у CGAP Brief, вище, зноска 46.

(c) полегшений контроль над небанківськими емітентами відповідно до принципу пропорційності контролю;
(d) можна очікувати, що зниження витрат на проведення транзакцій з використанням м-грошей призведе до більш значного зростання м-грошей (надання дозволу операторам мобільного зв'язку бути емітентами м-грошей, а не просто надавати мережеві послуги, може зменшити витрати, оскільки в противному випадку може бути більше сторін, задіяних у ланцюгу переказу, якщо оператори мобільного зв'язку самі не авторизовані бути емітентами м-грошей);
(e) заходи щодо зниження ризику, які, як правило, санкціоновані для небанківських емітентів (зокрема, мати на депозиті в установі, що перебуває під розсудливим наглядом, суму коштів, еквівалентну загальній сумі електронних грошей, випущених відповідним небанківським емітентом (тобто загальна сума електронних грошей, випущених небанківським емітентом, яка іноді називається «електронною касовою готівкою»);
(f) комерційно-технологічне становище, в якому знаходяться оператори мобільного зв'язку, що дозволяє випускати м-гроші;
(g) принципи консенсусу в цій області на основі пропорційних правил, спрямованих на регулювання видів послуг, а не на виявлення відмінностей між різними типами юридичних осіб[70].

99. Доцільно відзначити, що змінена версія Директиви ЄС про платіжні послуги (PSD2)[71], в поєднанні з Директивою про електронні гроші [72], як виявляється, не виключає можливості операторів мобільного зв'язку в якості емітентів мобільних грошей, але без звільнення їх від отримання дозволу у відповідності із законодавчо встановленими схемами авторизації для надання платіжних послуг.

Агенти з грошових переказів

100. Платіжні агенти відрізняються від небанківських емітентів в тому, що їх функція полягає в наданні платіжних послуг (також відомі як агенти з грошових переказів). Відповідно, на них не розповсюджується такий же рівень захисту. Як правило, таким агентам дозволяється зберігати кошти тільки протягом обмеженого періоду, і на відміну від небанківських емітентів, від них не вимагається виконувати вимоги щодо захисту грошових коштів. Це є тим аспектом, при якому регуляторний режим може сприяти розвитку м-грошей, забезпечуючи агентам, що надають

[70] Див. Загальний принцип 3 у публікації General principles for international remittance services, підготовленій Комітетом з платіжних і розрахункових систем Світового банку і Банку міжнародних розрахунків, стор. 4 (Розділ 1) та 17 (пункт 64) http://www.bis.org/cpmi/publ/d76.pdf
[71] Вище, зноска 13.
[72] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN.

фінансові послуги за допомогою мобільних телефонів, більш ліберальне нормативно-правове середовище.[73]

Вимоги до звітності

101. Небанківський емітент може бути зобов'язаний періодично звітувати перед контролюючим органом про наступні дані: кількість клієнтів, кількість нових рахунків, загальна сума невиплачених електронних грошей, загальна сума грошових переказів, кількість транзакцій, ліміти по транзакціям клієнтів і агентів (і кількість порушень лімітів), кількість і характер помилкових і нездійснених транзакцій, кількість скарг клієнтів, кількість і характер випадків шахрайства та порушення безпеки даних, кількість нових агентів і припинених агентських угод, а також кількість крадіжок в агентських точках.[74]

C. Захист прав споживачів

102. Різні види основних методів і захисних заходів, зазначених у Частині I цього документу, спрямовані, принаймні частково, на захист прав споживачів. У 2016 році Рада ОЕСР внесла зміни до Рекомендації Ради про захист прав споживачів в сфері електронної комерції для вирішення нових і виникаючих проблем, з якими стикаються споживачі.[75] Змінена рекомендація вирішує питання захисту прав споживачів з урахуванням нових подій в галузі електронної комерції[76]:

- *Негрошові транзакції* – обмін споживачів своїми персональними даними для «безкоштовних» товарів і послуг викликає побоювання у сенсі захисту їх прав;
- *Продукти цифрового контенту* – у цьому сенсі важливо, щоб споживачам надавалася чітка інформація про договірні умови їх доступу та будь-які відповідні обмеження щодо використання, а також про функціональність і сумісність таких продуктів;
- *Активні споживачі* – захист прав споживачів було поширено на транзакції споживач – споживач;
- *Мобільні пристрої* – використання таких пристроїв, з їх технологічними обмеженнями (зокрема, невеликий розмір екрану) впливає на розкриття інформації та облік, які є необхідними для захисту інтересів споживачів;
- *Ризики порушення конфіденційності та безпеки* – розширення ролі персональних даних в електронній комерції посилює ризики порушення конфіденційності та безпеки;

[73] Такий більш поблажливий регуляторний підхід центрального банку до м-грошових агентів можна побачити, наприклад, в Кенії (див. IFC Summary Report, вище, зноска 47, стор. 4).
[74] Цей список типів даних взятий з Supervising Nonbank E-Money Issuers, вище, зноска 46, стор. 3.
[75] Доступно на https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf.
[76] На підставі резюме в передмові до переглянутої версії Рекомендації ОЕСР, там же, стор. 4 та 5.

- *Захист платежів* – існує потреба в розширенні захисту інтересів споживачів за допомогою різних механізмів оплати;
- *Безпека продукту* – ризики безпеки споживачів підвищуються з появою в Інтернеті заборонених або відкликаних продуктів.

103. Зважаючи на вищезазначене, змінена Рекомендація висвітлює різні пріоритетні кроки щодо захисту прав споживачів, наприклад:

- Компанії не повинні спотворювати або приховувати умови, які можуть вплинути на рішення споживача щодо транзакції (№ 5);
- Необхідність для бізнесу не займатися шахрайськими діями, пов'язаними зі збиранням і використанням персональних даних споживачів (№ 8);
- Реклама за участю відомих особистостей повинна бути правдивою, обґрунтованою і відображати думки та реальний досвід таких особистостей (№ 17);
- Компанії повинні розробити і впровадити ефективні та прості у використанні процедури, які дозволяють споживачам вибирати, чи хочуть вони отримувати небажані рекламні повідомлення, чи то електронною поштою, чи то за допомогою інших електронних засобів (№ 22);
- Розкриття інформації в Інтернеті повинне бути чітким, точним, легко доступним і помітним, щоб споживачі мали достатню інформацію для прийняття обґрунтованого рішення щодо транзакції (№ 25);
- Компанії повинні надавати споживачам чітку та повну інформацію про відповідні умови транзакції (№ 34);
- Компанії повинні забезпечити, щоб момент, в який споживачів просять підтвердити транзакцію, після якого наступає строк платежу або вони іншим чином зв'язані договірними зобов'язаннями, є чітким і однозначним, так само як і кроки, необхідні для здійснення транзакції, особливо для нових механізмів оплати (№ 36);
- Компанії повинні давати можливість споживачам зберігати повну, точну і довговічну документацію про транзакцію, в форматі, сумісному з пристроєм або платформою, які споживачі використовували для здійснення транзакції (№ 39);
- Споживачі повинні мати доступ до альтернативних механізмів вирішення суперечок, включаючи онлайнові системи вирішення суперечок, з метою сприяння врегулюванню претензій щодо транзакцій у сфері електронної комерції, з особливою увагою до транзакцій на невеликі суми або транскордонних транзакцій. Незважаючі на те, что такі механізми можуть фінансуватися у різні способи, вони повинні бути призначені для забезпечення вирішення суперечок на об'єктивній, неупередженій та послідовній основі, при цьому результати вирішення індивідуальних суперечок повинні бути незалежними від впливу з боку тих, хто надає фінансову або іншу підтримку (№ 45).

104. Різні заходи щодо захисту прав споживачів, які стосуються сфери електронної комерції, включені в останню Директиву ЄС про захист прав споживачів.[77] Ці заходи, зокрема, включають в себе:

- Детальні вимоги щодо розкриття інформації споживачам до укладання договору (стаття 6);
- Посилання на необхідність включення розкриття інформації з урахуванням технічних обмежень деяких засобів масової інформації (наприклад, обмежений розмір екрану мобільного телефону) (стаття 8.4);
- Право відмови, в разі «дистанційного контракту», від транзакції протягом 14-денного терміну, розрахованого відповідно до правил, встановлених в Директиві (з подовженням цього терміну до 12 місяців, якщо трейдер не розкрив споживачеві інформацію про право відмови (стаття 9);
- У зв'язку з правом відмови споживача (з урахуванням ряду винятків, зазначених у Директиві), зобов'язання трейдера відшкодувати ціну покупки, включаючи витрати на доставку (але не додаткові витрати, якщо споживач зробив вибір на користь термінової доставки) (стаття 13);
- Створення зразкової форми відмови;
- Деякі витрати, які не можуть бути перекладені на споживача, якщо вони не розкриті належним чином (стаття 6.6);
- Вимоги до розкриття інформації, особливо ті, що стосуються сфери електронної комерції, в тому числі наслідки натискання клавіши комп'ютерної миші для прийняття умов угоди (стаття 8.2).

105. Директива ЄС про права споживачів (стаття 8(4))[78] містить положення, в якому розглядається ситуація з передачею інформації в зв'язку з укладанням дистанційного контракту на мобільний пристрій з обмеженим обсягом пам'яті. Якщо контракт укладений за допомогою засобу дистанційного зв'язку, який дозволяє обмежений простір або час для відображення інформації, трейдер повинен забезпечити, на цьому конкретному засобі, до укладання такого контракту, принаймні передконтрактну інформацію про основні характеристики товарів або послуг, особистість трейдера, загальну вартість контракту, право відмови від контракту, термін дії контракту та, якщо контракт має невизначений термін, умови розірвання контракту.

D. Врегулювання суперечок

106. В тій чи іншій мірі, правові рамки для електронної комерції передбачають розгляд питання про врегулювання суперечок. Як зазначено у цьому документі, легкодоступні механізми врегулювання суперечок (наприклад, онлайнові

[77] Вище, зноска 11.
[78] Див. зноску 11 вище.

механізми вирішення спорів) є ключовим елементом. Врегулювання суперечок в режимі онлайн, як правило, розуміється як застосування різних видів альтернативних механізмів вирішення спорів.

107. Врегулювання суперечок в режимі онлайн охоплює низку можливих механізмів позасудового вирішення спорів, в тому числі врегулювання в режимі онлайн на основі використання спеціалізованих експертів, які займаються врегулюванням фінансових претензій, арбітражем, беруть участь у роботі комісій з розгляду скарг споживачів, примиренням і посередництвом.

108. Відповідно до Директиви ЄС 2013/11/ЄС про альтернативне вирішення спорів зі споживачами і пов'язаним з нею Регламентом ЄС про врегулювання спорів за участю споживачів в режимі онлайн, трейдери, які зобов'язані використовувати альтернативне вирішення спорів, повинні розкрити інформацію про це своїм клієнтам і вказати посилання на платформу ЄС щодо врегулювання спорів в режимі онлайн. Компетентні органи в кожній державі-члені оцінюють суб'єкти альтернативного вирішення спорів у своїх країнах відповідно до стандартів якості, встановлених у Директиві, і подають Комісії свої списки національних органів з альтернативного вирішення спорів. Трейдери, які вирішили використовувати альтернативне вирішення спорів, зобов'язані розмістити посилання на платформу врегулювання спорів в режимі онлайн на своїх сайтах.

109. Комісія ЄС створила інтерактивну, багатомовну платформу врегулювання спорів в режимі онлайн (**http://ec.europa.eu/odr**) з метою сприяння врегулюванню контрактних суперечок щодо купівлі товарів та послуг в режимі онлайн за допомогою альтернативного вирішення спорів.[79] Ця платформа полегшує подачу скарг в режимі онлайн (будь-якою мовою країн ЄС) і вибір органу з альтернативного вирішення спорів з числа тих, що зареєстровані у платформі, а також передачу в орган з альтернативного вирішення спорів для винесення рішення. Більше того, платформа врегулювання спорів в режимі онлайн дозволяє вирішення спорів в режимі онлайн. Країни-члени зобов’язані створити національні контактні пункти для надання допомоги користувачам платформи врегулювання спорів в режимі онлайн.

[79] http://ec.europa.eu/consumers/solving_consumer_disputes/non-judicial_redress/adr-odr/index_en.htm; у цьому відношенні, див. Регламент (ЄС) No 524/2013 (21 травня 2013 р.) про врегулювання спорів за участю споживачів в режимі онлайн; цей Регламент вимагає від Комісії створити платформу врегулювання суперечок в режимі онлайн на рівні ЄС; доступно на http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0001:0012:en:PDF.