

their types to certain groups in accordance with the type and scope of activities of financial institutions.

References:

1. “On Financial Services and State Regulation of Financial Services Markets” :Law of Ukraine 12.07.2001 № 2664-III // <http://zakon2.rada.gov.ua/laws/>
2. «On Banks and Banking Activities» Law of Ukraine: 07.12.2000, № 2121-III // <http://zakon2.rada.gov.ua/laws/>
3. “Civil Code of Ukraine Law of Ukraine”: 16.01.2003 № 435-IV// <http://zakon2.rada.gov.ua/laws/>
4. “Economic Code of Ukraine Law of Ukraine”: 16.01.2003 № 436-IV // <http://zakon2.rada.gov.ua/laws/>
5. “Budget Code of Ukraine”:Law of Ukraine 24.12.2010 // <http://zakon2.rada.gov.ua/laws/>
6. “On Payment Systems and Transfer of Funds in Ukraine”: Law of Ukraine 05.06.2001 // // <http://zakon2.rada.gov.ua/laws/>

DOI <https://doi.org/10.30525/978-9934-588-92-1-71>

СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА УПРАВЛІННЯ РИЗИКАМИ ЛЕГАЛІЗАЦІЇ КОШТІВ

Сосенко В. М.

*аспірант кафедри господарського та адміністративного права
Національного технічного університету України «Київський
політехнічний інститут імені Ігоря Сікорського»
м. Київ, Україна*

Дистанційне надання фінансових послуг на сьогодні є вкрай актуальним, що зумовлено як розвитком технологій так і соціальним дистанціюванням через пандемію. З розвитком інтернет-технологій прямо пропорційно збільшуються і види кіберзлочинів серед яких соціальна інженерія [1, с. 214], а використання новітніх технологій для відмивання коштів/фінансування тероризму має високий ризик через використання дистанційних послуг [1, с. 233]. Інформаційно-телекомунікаційні та комп'ютерні технології досягли рівня, що спрощують процеси отримання ідентифікаційної інформації та дозволяють верифікувати особу, водночас із тим, обмежуючи фізичне сприйняття

особистості клієнта, візуальний аналіз документів, поданих ним, що може бути підґрунтям для неправомірного використання послуг фінансової установи з протиправною метою. Заходами належної перевірки, є ідентифікація та верифікація клієнта, обсяг дій при здійсненні кожного із заходів належної перевірки визначається суб'єктом первинного фінансового моніторингу, з урахуванням ризик-профілю клієнта [2], при цьому, нормотворцем відеоверифікація визначається повноцінною моделлю верифікації.

Віддалене встановлення ділових відносин та відеоверифікація як процедура здійснення банком верифікації особи в режимі відеотрансляції [3] містять у собі ризик можливого використання фінансової установи з метою легалізації коштів/ фінансування тероризму, зокрема, через приховування фактичної особи, в інтересах якої або від імені якої буде здійснена фінансова операція. Так, у режимі відео трансляції можливе надання та отримання ідентифікаційних даних: власних – реальною особою, що вимушено, через неправомірний тиск третьої особи, примушується до скористання послугою фінансової установи; або реальних даних – «фейковою» особою, яка володіє ними та які отримані завдяки фішингу, вішингу, прітекстингу, тощо, тобто завдяки методам соціальної інженерії. І завдяки цим же методам може здійснюватися вплив на працівника фінансової установи, з метою отримання відповідної послуги, оскільки режим відео трансляції не позбавляє процес верифікації суб'єктивних людських психологічних складових. При цьому, абсолютно реальним постає питання поєднання шахрайства, пов'язаного з крадіжкою персональних даних, із відмиванням коштів/фінансуванням тероризму, і, відповідно, управління ризиками, в площині їх мінімізації, через своєчасне виявлення методів соціальної інженерії під час встановлення ділових відносин є реальним заходом попередження/виявлення кримінально карного діяння.

Соціальна інженерія – сукупність методів використання психологічних особливостей особи з метою спонукання її до певних дій, яких би вона за звичних умов не вчинила, введення особи в оману [3, 4]. Соціальну інженерію розглядають як незаконний метод отримання інформації, тому сьогодні її активно використовують в інтернеті для отримання закритої інформації або інформації, яка являє велику цінність [5, с. 34]. Соціальна інженерія – це метод несанкціонованого доступу до інформаційних ресурсів, що ґрунтується на особливостях психології людини [6, с. 64]. Відеоверифікація, але не виключно вона, може стати інструментом для шахрайського впливу на працівника фінансової установи, тому уповноважений працівник банку/установи під час здійснення відеоверифікації має пересвідчитися в тому, що немає ознак тиску/впливу на особу, верифікація якої здійснюється, третьою особою.

У разі наявності ознак такого тиску, працівник має детальніше розпитати особу про мету встановлення ділових відносин для зниження ризику подальших шахрайських дій за допомогою соціальної інженерії [3, 4]. Звертає увагу на себе те, що основним способом захисту від методів соціальної інженерії є навчання працівників [6, с. 67], яке не повинно бути формальним, та зводиться до ознайомлення з внутрішніми положеннями суб'єкта, воно має бути систематичним, та таким, що базується на сучасному досвіді та здійснюватися в практичній площині.

Окрім того, вважаємо за доцільне, залежно від ризик-профілю клієнта, використовувати комбіновану модель верифікації, поєднавши відеоверифікацію з іншою самостійною моделлю верифікації – верифікацією за допомогою BankID НБУ та кваліфікованого електронного підпису, закріпивши таку модель верифікації у внутрішніх нормативних документах суб'єкта первинного фінансового моніторингу. Така модель, також суттєво знизить ризик суб'єктивного сприйняття – оцінки на власний розсуд працівником суб'єкта первинного фінансового моніторингу, що здійснює відеоверифікацію, як особи так і документів, що верифікуються в такий спосіб.

Таким чином, урахувавши, що методи соціальної інженерії можуть застосовуватися при здійсненні відеоверифікації, а нормативно-правові акти з питань фінансового моніторингу повною мірою не врегульовують питання протидії та управління ними, а містять лише загальні положення щодо загроз їх наявності, цю модель верифікації слід розглядати як таку, що несе ризики, однак вони є такими, що піддаються управлінню. Основними напрямками належного регулювання щодо управління ними можна визначити: розробка спеціальних методик виявлення та реагування на використання методів соціальної інженерії, закріплення їх у внутрішніх документах з питань фінансового моніторингу, у формі деталізованого опису заходів (правове регулювання); включення до програми навчання працівників суб'єкта первинного фінансового моніторингу, що задіяні у процесах відеоверифікації, відповідних методик та систематичне практичне їх навчання.

Література:

1. Звіт про проведення національної оцінки ризиків у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, та фінансуванню тероризму 2019. URL: <https://finmonitoring.in.ua/NRA2019.pdf> (дата звернення 19.10.2020);
2. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення, Закон України 6

грудня 2019 року № 361-IX. URL: <https://zakon.rada.gov.ua/laws/show/361-20?find=1&text#Text> (дата звернення 19.10.2020).

3. Про затвердження Положення про здійснення банками фінансового моніторингу Постанова Національного банку України 19.05.2020 № 65. URL: <https://zakon.rada.gov.ua/laws/show/v0065500-20#Text> (дата звернення 19.10.2020).

4. Про затвердження Положення про здійснення установами фінансового моніторингу Постанова Національного банку України 28.07.2020 № 107 URL: <https://zakon.rada.gov.ua/laws/show/v0107500-20#Text> (дата звернення 19.10.2020).

5. Бортник, С. М. Соціальна інженерія як метод вчинення злочинів / Сергій Миколайович Бортник // Протидія кіберзагрозам та торгівлі людьми: зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 26 листоп. 2019 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. – Харків : ХНУВС, 2019. – С. 34-35. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/6425/Sotsialna%20inzheneriia%20yak%20metod%20vchynenni%20zlochyniv_Bortnyk%20S_2019.pdf?sequence=1&isAllowed=y (дата звернення 19.10.2020).

6. Протидія злочинам, що вчиняються за допомогою методів соціальної інженерії в інтернеті / Ю. М. Онищенко, К. Е. Петров, І. В. Кобзев // Право і Безпека. – 2017. – № 1. – С. 63-68. URL: http://nbuv.gov.ua/UJRN/Pib_2017_1_13 (дата звернення 19.10.2020).

DOI <https://doi.org/10.30525/978-9934-588-92-1-72>

ДО ПИТАННЯ РЕГУЛЮВАННЯ ТЕХНОЛОГІЇ ОТТ У СФЕРІ АУДІОВІЗУАЛЬНИХ МЕДІА ПОСЛУГ В УКРАЇНІ

Шрам Є. О.

студентка магістратури другого року навчання

Інституту права

Київського національного університету імені Тараса Шевченка

м. Київ, Україна

Технологія over-the-top (ОТТ) – технологія доступу до програмного продукту, що дозволяє кінцевим користувачам отримувати різноманітний вміст, зокрема аудіовізуальний, в режимі реального часу незалежно від мереж операторів та провайдерів телекомунікаційних послуг завдяки підключенню до мережі Інтернет. За визначенням