координування графіків руху. Іншими словами перспективи розвитку контрейлерних перевезень АТ «Укрзалізниці» лежать в площині власне мультимодальних перевезень.

Для успішного розвитку контрейлерних перевезень в Україні існує необхідність проведення заходів, які б охоплювали наступні аспекти: технічні, технологічні, організаційні, нормативно-правові. Ґрунтуючись на зазначених у [1] напрямах реформування АТ «Укрзалізниця» вкрай нагальним постає питання розширення термінальної бази для обробки вантажів із застосуванням сучасних логістичних технологій, що дозволило би надавати власникам автотранспортних засобів та вантажів більш широкий та якісний спектр послуг. Цікавим є досвід США, де існує 14 видів контрейлерного транспортування й найбільшим попитом користується спосіб «знімний кузов», що відбувається за схемою «автомобільні шасі – залізнична спеціалізована платформа – автомобільні шасі». Такий підхід має перевагу у порівнянні із транспортуванням автомобіля на платформі щодо меншої ваги, а відтак й навантаження на осі є значно меншим. Але знімний кузов має значно меншу міцність, що забезпечує менший захист при транспортуванні і не допускає штабелювання.

Такі нововведення на рівні держави дадуть екологічний, соціальний ефект, а також економію коштів державного бюджету через менші витрати на відновлення автошляхів. На рівні вантажовласника такий вид комбінованих перевезень дасть можливість прискорити оборотність капіталу через скорочення грошових витрат і витрат часу на процес транспортування, а також зниження ризику.

1. Стратегія АТ «Укрзалізниця» на 2019-2023 роки URL: https://uz.gov.ua/files/file/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%8F-4-Typography.pdf.

2. Економічна статистика / Економічна діяльність / Транспорт URL: http://www.ukrstat.gov.ua/operativ/menu/menu_u/tr.htm.

3. A. Vasilis Vasiliauskas, I. Kabashkin. Analysis of Indicators Measuring Performance of Rail-Road Terminals / Proceedings of 10'th International Conference. Transport Means. 2006, pp. 93-96.

Семенченко Н.В., Васильченко І.В.
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БАНКІВСЬКОЇ БЕЗПЕКИ В УКРАЇНІ

Актуальність: Банківська система є однією з основних складових у фінансовій системі держави. Згідно з думкою автора, вимоги банківської системи можуть отримувати статус державної політики в сфері фінансової діяльності, а діяльність банків не можна розглядати у відриві від виробництва, обігу та споживання матеріальних благ, від політики, ідеології, культури, освіти, соціальних та етичних орієнтирів, якими керуються члени суспільства [1]. Через це можна стверджувати, що рівень безпеки банківської діяльності повинен бути надзвичайно високим, оскільки будь-які загрози можуть як зашкодити стабільній банківській роботі, так і навіть повністю її призупинити, що безпосередньо вплине на роботу інших сфер держави.

Для повного та коректного дослідження обраної теми надамо визначення такому поняттю, як «банківська безпека». Варто зазначити, що не існує єдиного визначення наведеному поняттю, тому автори намагаються надати йому власне визначення та виокремлюють у ньому різні складові, які його формують [2-3]. Наведемо декілька прикладів. А.Р. Алавердов виокремлює три основних компоненти безпеки сучасної кредитно-фінансової організації [5, с. 6]: інформаційна безпека банку, безпека персоналу банку та майнова безпека банку. М. Зубок [6, с. 10] розрізняє такі види безпеки банківської діяльності: особисту, колективну, економічну та інформаційну.

Таким чином, можна виділити деякі складові банківської безпеки, що найбільш повторюються, та надати їм таку класифікацію: безпека працівників, безпека матеріальних ресурсів та інформаційна безпека. Проаналізуємо кожну з представлених складових.

Безпека працівників – означає забезпечення комфортної та стабільної праці, а також відсутність загроз для працівників банку [2, с.22]. Цього можна досягти дотримуючись встановлених правил поведінки, а також залучивши фізичну охорону, чи засоби охорони, для відділень банку, а також на місця можливої загрози для працівників.

Безпека матеріальних ресурсів – це захищеність від будь-яких загроз грошових коштів, цінних паперів, матеріальних цінностей [2, с. 22]. Це забезпечується так само як і безпека працівників, залучаючи професійні засоби охорони, для попередження та усунення загрози.

Інформаційна безпека – це забезпечення безперебійного функціонування банківських систем, що збирають та оброблюють інформацію, захист від розповсюдження комерційної інформації про клієнтів, а також від джерел інформації [2, с. 22-24]. Для цього створені комп'ютеризовані системи захисту, певні процедури обробки та зберігання даних. Також працюють служби безпеки банків, які відстежують дії працівників на предмет неправомірних операцій, що можуть зашкодити безпеці банку. Крім цього, регулярний моніторинг системи на наявність вразливих частин.

Таким чином, можна виділити, що безпека працівників та безпека матеріальних ресурсів передбачає фізичну охорону, в якій мала частка інноваційних технологій (насамперед, це ті технології, які банк не може впроваджувати, оскільки цим повинні займатися охоронні компанії, які працюють на замовлення банку). Найбільш актуальним та доречним буде розгляд інноваційних технологій, що забезпечують інформаційну безпеку банку.

Отже, перейдемо до систем інформаційної безпеки банку. О.І. Барановський у своїй роботі наводить наступне пояснення інформаційної безпеки – це система заходів захисту банків від витоку конфіденційної інформації, насамперед, про клієнтів. Це досягається внаслідок забезпечення наступних принципів безпеки: доступності, цілісності, конфіденційності. Інструментарій включає технічні роботи, процеси управління персоналом, організаційну й адміністративну підтримку, регулярну оцінку ризиків. Окрім цього, згадується про банківську таємницю. Це обов'язок банку зберігати у таємниці дані про клієнтів та стан їх рахунків, а також виконуванні ними операції. [2, с. 25]

Як згадував автор, банківська таємниця – має різні аспекти, а саме правові, соціально-економічні, політичні, міжнародні, психологічні та етичні. Наприклад, в разі виявлення нелегальних способів отримання прибутку особою, нею стають зацікавлені правоохоронні органи. Це за собою тягне розкриття банківських операцій, що проводилися на рахунку вищезазначеної особи. Існує також варіант зловживання владою посадових осіб, що означає можливість отримання конфіденціальної інформації від банку про проведені операції конкурента. Тому банківська таємниця є досить важливим фактором у функціонуванні банку та, зокрема, інформаційній банківській безпеці. Після підписання «Конвенції ООН про боротьбу проти незаконного обігу наркотичних засобів і психотропних речовин», держави – учасниці зобов'язалися пом'якшити режим банківської таємниці, щодо справ пов'язаних з оборотом наркотичних та психотропних речовин. Однак інші операції з «брудними» грошима, що випливають з інших неправових дій, згаданої конвенції не торкаються, зокрема порушення щодо сплати податків. Згідно зі Страсбурзькою угодою – «Конвенцією Ради Європи про відмивання, пошук, арешт і конфіскацію доходів, одержаних злочинним шляхом, та про фінансування тероризму», держави зобов'язалися розкривати банківську таємницю не лише у сфері наркоторгівлі, а й в інших сферах кримінальної діяльності. Окрім цього, обов'язок з розкриття банківської таємниці в зазначених ситуаціях не діє, якщо мова йде про підозру в протиправних вчинках відносно обрахування та сплати податків, тобто таких, що розслідуються податковими та фінансовими відомствами. [2]

Виходячи з вище згаданої проблеми, запропонуємо інноваційну технологію захисту від витоку конфіденційної інформації про клієнта назовні, але даний метод матиме можливість отримання даних в разі законної вимоги встановлених органів. Метод має 4 пункти:

Заборонено добувати з системи, де зберігаються дані, та поширювати будь-яку конфіденційну інформацію про клієнта, окрім випадків передбачених цими пунктами та законодавством України;

У разі службової необхідності, для перевірки даних клієнта – дані клієнта вводяться в систему, а вона, в свою чергу, видає дані про те, чи є цей клієнт у системі, та надає інформацію про достовірність наданих даних, наприклад, прізвище, ім'я, по батькові, дата народження, номер паспорту, реєстраційний номер облікової картки платника податків, фото клієнта тощо. Тобто дані не можна отримати з системи, а можна лише вводити їх в систему на перевірку достовірності;

У випадку, коли дані необхідно саме отримати з системи (згідно з законодавством України, в тому числі Закон України «Про банки і банківську діяльність» [8]), то відбувається процедура з участю декількох працівників з різних відділів (в ідеалі – випадковим чином), аби зменшити корупційні ризики. Кожен з працівників розглядає необхідність отримання цих даних, та, у разі позитивного рішення, надає власний, наприклад, унікальний цифровий підпис для отримання даних від системи. Якщо хоча б один з тих осіб, що перевіряють необхідність доступу, нададуть інформацію про те, що доступ до цих даних є неправомірним, то цю спробу буде відхилено, а також буде проведена додаткова перевірка, щодо правомірності доступу;

Кожна подібна операція зберігається та відправляється службі безпеки банку, яка може розглядати подібні операції на предмет витоку конфіденційної інформації про клієнта. Та у разі виявлення такої проблеми – своєчасно можна буде вживати заходи по усуненню цієї загрози.

У свою чергу, кожен з працівників буде нести відповідальність за неправомірні дії, тобто у випадку несанкціонованого доступу, або навпаки, коли була необхідність в отримані даних, але була відмова у доступі. Також необхідно зауважити, що залучати працівників до даної процедури варто лише тих, хто пройшов певну підготовку, оскільки непідготовлений працівник буде нести загрозу безпеці банку.

А також, щодо корупційних ризиків, згаданих у 3-му пункті, то можна навести нескладний приклад, що демонструє працездатність методу. Нехай кожен з працівників має ймовірність 0,01 того, що його зможуть «підкупити» аби неправомірно отримати дані з системи (тобто 1% на підкуп). Якщо у вище згаданій процедурі буде брати участь лише 1 працівник, то ймовірність витоку комерційної інформації буде складати 0,01 (або 1%), але якщо таких працівників буде 3, та ми будемо вважати, що ймовірність «підкупу» цих працівників не залежить один від одного, то за теоремою «про незалежну ймовірність», ймовірність витоку подібної інформації буде складати $1*10^{-6}$ (або 0,0001%) що значно підвищує безпеку банку [9, с. 16].

Однак система банківської безпеки повинна будуватися не лише на комп'ютерних системах, а повинна бути комплексною та системною.

Висновок: банківська безпека в Україні є дуже важливою, оскільки маючи слабку систему забезпечення функціонування банків, держава ризикує зупинити банківську систему, а у зв'язку з цим зупиниться також інші сфери державної діяльності. Зокрема, інформаційна безпека в банках є головною, оскільки в наш час важливо як володіти цінною інформацією, так і захищати від незаконного посягання на неї. Окрім цього, варто системно підходити до забезпечення банківської безпеки, мати актуальні способи захисту від різних загроз та впроваджувати інноваційні технології для того, аби бути на крок попереду від недобросовісних осіб, бажаючих незаконно заволодіти чужим майном, або інформацією, яка є недоступна для них.

1. Онищенко Ю.І. Банківська система як складова фінансової системи. Науковий вісник. Одеський державний економічний університет. Всеукраїнська асоціація молодих науковців. Науки: економіка, політологія, історія. 2009. №8 (86). С. 95-104.

2. Барановський О. Безпека банківської сфери. Вісник Національного банку України. 2014. № 6. С. 20-27. Режим доступу: http://nbuv.gov.ua/UJRN/Vnbu_2014_6_9.

3. Лелюк Н.Є., Родченко С.С. Ідентифікація загроз фінансовій безпеці банків. 2019. URL: http://journals.uran.ua/tarp/article/download/168431/171600

4. Гребенюк Н.О. Фінансова безпека банків: система розпізнавання загроз та усунення ризиків. Вісник Харківського національного університету імені В. Н. Каразіна. Економіка. 2016. № 91. С. 53-64.
5. Алавердов А.Р. Организация и управление безопасностью в кредитнофинансовых организациях: Учебное пособие. М.: Московский государственный университет экономики, статистики и информатики, 2004. 82 с.
6. Зубок М.І. Безпека банків: навч. посіб. К.: КНТЕУ, 2002. 306 с.
7. Зубок М.І. Безпека банківської діяльності: навч. посіб. К.: КНЕУ, 2002. 190 с.
8. Про банки і банківську діяльність: Закон України від 7 грудня 2000 року. № № 2121. URL: http://zakon1.rada.gov.ua/laws/show/2121-14 (дата звернення: 30.04.2020).
9. Каніовська І.Ю. Теорія ймовірностей у прикладах і задачах: навч. посіб. Київ, 2002. 168 с.

Строгуш Ю.Б.
Львівський національний університет імені Івана Франка
Огінок С.В.
Національний університет «Львівська політехніка»

УПРАВЛІННЯ ІННОВАЦІЙНИМ ПРОЦЕСОМ В УКРАЇНІ: СОЦІАЛЬНЕ ПІДПРИЄМНИЦТВО

Соціальна діяльність, як інноваційний процес починає формуватися на території України. Своєю діяльністю соціально-орієнтовані підприємства генерують соціальні інновації, котрі можуть принести користь для різних зацікавлених сторін: для бізнесу – зростання доходів і прибутків, обсяг клієнтів, лояльність і задоволеність, ділова репутація; для соціальних цільових груп – скорочення безробіття та соціального відторгнення соціальних цільових груп; для держави сприятливу громадську думку та збільшення її іміджу [8].

Вже другий рік поспіль я досліджую тему соціального підприємництва і можу запевнити, що саме такі підприємства можуть допомогти розвитку країни. Враховуючи ситуацію, в якій зараз перебуває Україна, соціальне підприємництво для нас стає ще більш актуальним. Соціальні підприємства допомагають вирішувати питання з безробіттям, захисту навколишнього середовища, питання пов'язанні з освітою, культурою, наукою тощо.

Діючі в Україні соціальні підприємства наразі сильно відрізняються від закордонних аналогів, оскільки їх діяльність має багато нюансів. Практично за кожним з них стоїть якийсь фонд або гранти, адже щоб почати бізнес, потрібен стартовий капітал. Досягнення прибутковості для більшості компаній, що займаються соціальним підприємництвом, – мета далекої перспективи: їх поточні завдання більшою мірою стосуються виконання соціальних програм, а не розробки ефективних бізнес-підходів [2].

Соціальне підприємництво в нашій державі часто є єдиним можливим варіантом бодай часткового вирішення суспільних проблем. Для його сталого розвитку виникає необхідність сприятливого клімату, який повинні створити уряд і місцева влада. Уряд має чітко усвідомлювати, що соціальне підприємство є інструментом, який сприяє розвитку суспільства. Головним завданням, у контексті цього, стає подолання недостатньої обізнаності щодо його природи, брак нормативно-правової бази, що регулювала б діяльність соціальних підприємств, а також незначний обсяг інформації в ЗМІ про діяльність численних соціальних підприємців [2]. Слід також звернути увагу на те, що на сьогодні українські вищі навчальні заклади недостатньо активні у справі включення соціального підприємництва в освітянські програми, що призводить до того, що українські студенти не одержують інформації про роль соціального підприємництва для розвитку громадянського суспільства і про можливість, що воно відкриває для їх особистої реалізації. Це породжує відсутність системного підходу до виховання та підготовки кваліфікованих кадрів для здійснення діяльності у сфері соціального підприємництва [4].

Для активізації розвитку соціального підприємництва в Україні потрібне:

– прийняття закону про соціальне підприємництво, яким було б визначено чіткі критерії соціального підприємництва та створено правові механізми підтримки соціальних підприємців;