УКД 336.717.061(477)

Т.С. Шалига, *АТ "Сведбанк", м. Київ*

РЕГУЛЮВАННЯ ПОРЯДКУ РОБОТИ З ІНФОРМАЦІЄЮ ПРИ БАНКІВСЬКОМУ ДИСТАНЦІЙНОМУ ОБСЛУГОВУВАННІ

Дистанційні послуги як сучасний прогресивний продукт банківської діяльності вимагає модернізованого врегульованого підходу при впровадженні. Банківська інформація як основний об'єкт оперування при дистанційному обслуговуванні вимагає захисту на законодавчому, технологічному та процедурному рівнях. У статті досліджено аспекти багатофакторного убезпечення інформації з метою мінімізації низки банківських ризиків.

Ключові слова: дистанційне банківське обслуговування, інформаційна безпека, інформаційні банківські ризики.

Розвиток альтернативних банківських послуг в Україні є одним із показників інтеграції національної банківської системи у світову економіку. Окрім того, інтенсивне використання інформаційних технологій на ринку банківських послуг підвищує конкурентні показники окремих інститутів та є виразним індикатором спроби відродження фінансового сектора, пригніченого за наслідками світової економічної кризи.

Постановка проблеми. Дистанційні послуги є специфічним продуктом банківської діяльності і як звичайний продукт потребують впровадження цілого комплексу процедур, узгодження і врегулювання яких забезпечуватимуть позитивний ефект при винесенні цього продукту на ринок. Втім, специфіка дистанційного обслуговування передбачає використання низки нетрадиційних методів, що вимагає врегулювання чисельних бізнес-процесів, які супроводжують взаємодію банку зі споживачем. Побудова коректної комунікації, яка відбувається через дистанційні канали, тобто з віддаленою участю клієнта банку, спирається на глибокий структурований захист насамперед інформації, що передається.

Аналіз останніх досліджень і публікацій. Інформаційний аспект взаємодії банків з клієнтами регулюється низкою національних законодавчих актів, серед яких закони України "Про інформацію", "Про банки і банківську діяльність", "Про захист персональних даних", Про звернення громадян" та низка роз'яснень до них. А втім, законодавчі питання управління інформаційною діяльністю аж ніяк не вичерпують кола питань, які виникають у стратегічній та поточній діяльності банківських установ щодо роботи з інформацією. Дослідженню технологій адміністрування та захисту інформації присвячено роботи українських та іноземних дослідників і науковців: В. К. Галіцина, Г.Я. Яніловської, А.П. Колесника, В. М. Антонова, Н.І. Костіної. Також система комунікації банківської установи широко розглядається в організаційно-правовому аспекті, де прикладне використання законодавчої бази аналізується в межах внутрішньої інфраструктури. Цьому присвячено роботи Б.А. Кормича, І.Л. Бучило,

Л.В. Туманової, М.В. Якушева, М. Галамби, В. Петрика та багатьох інших. Значну увагу в контексті роботи банків з інформацією приділено питанням ризиків, що виникають у супутніх процесах, що досліджувалися в роботах Н.Є. Селюченко, В.П. Кічор, Т.Л. Мостенської.

Не вирішена раніше частина загальної проблеми. Захист інформації при передаванні її осучасненими технічними засобами неважко реалізувати на рівні програмно-апаратного рішення, розмаїття яких сьогодні представлено на ринку інновацій та активно використовується в банках. Проте регламентація процедур розголошення інформації респондентам при обслуговуванні їх дистанційними каналами, а також порядок використання банками інформації, накопиченої в ході роботи, на сьогоднішній день недостатньо реалізована та потребує суттєвого доопрацювання.

Урегулювання аспектів роботи з інформаційними даними при дистанційному обслуговуванні має визначатися на рівні внутрішніх процедур установи, формалізованих та узгоджених у межах технології та бізнес-процесів банку, а також на державному рівні з метою захисту інтересів населення та суб'єктів господарювання щодо убезпечення використовуваної інформації.

Метою статті є пошук гармонізованого співвідношення методів державного впливу на банківську систему щодо інформаційної діяльності суб'єктів останньої та результуючої побудови банками цілісної та послідовної програми заходів щодо оптимальної, захищеної та ефективної комунікації з клієнтами. Саме такий симбіотичний підхід сприятиме розвитку прогресивних, затребуваних ринком банківських послуг, якими є дистанційні технології обслуговування.

Виклад основного матеріалу. Інформаційна безпека – складна соціально-економіко-політична категорія, яка в контексті стрімкої інформатизації суспільства набуває все нових ознак і вимагає глибокого вивчення та особливого підходу щодо цілісної державно-інституціональної програми. З огляду на суб'єктів ринково-суспільних відносин, які використовують інформацію у своїй діяльності або повсякденному житті, інформаційну безпеку можна розглядати на мікрорівні та на макрорівні.

Реалізація заходів інформаційної безпеки на макрорівні передусім передбачає забезпечення конституціональних принципів обміну інформацією між членами суспільства, а також захист інформації в інтересах держави. При цьому концепція національної інформаційної політики має узгоджуватися з принципами міжнародного права. Безпека інформації безпосередньо пов'язана з впровадженням і використанням інформаційних технологій, які забезпечують контрольований комплекс процесів з її накопичення, розповсюдження та захисту від несанкціонованого доступу до неї.

Банківська діяльність тісно пов'язана з використанням інформації та охоплює як макрорівневий аспект у контексті забезпечення функцій національної банківської системи, так і мікрорівневий аспект у частині

діяльності установи як суб'єкта економічних відносин. Отже, доцільно розглядати роботу з інформацією, що проводить банк у ході надання послуг своїм клієнтам, у двох площинах.

На законодавчому рівні роботу з інформацією в Україні врегульовано насамперед Законом України "Про інформацію", затвердженим 2 жовтня 1992 року Постановою № 2657-XII. Даним законом введено термінологічні засади для визначення інформації такою, що підлягає обмеженому доступу, а саме її класифіковано на таємну та конфіденційну.

Банківські установи в ході своєї діяльності стають розпорядниками та мультиплікаторами численних інформаційних масивів різного формату та призначення, для кожного з яких має бути встановлений окремий контрольований режим використання. Важливість урегулювання процесів роботи з інформацією в банках має коріння насамперед у конфіденційному характері даних, котрими розпоряджається банківська інституція.

Конфіденційна інформація характерна тим, що може бути розповсюджена тільки з дозволу та в порядку, узгодженому з власником інформації. Відтак у межах банківської діяльності угода банку з клієнтом і є тим фіналізуючим документом, який передбачає порядок використання інформації. У той же час інформація про клієнтів та пов'язана з обслуговуванням клієнтів також є і таємною інформацією, оскільки містить банківську таємницю. Частиною 1 ст. 60 Закону України "Про банки і банківську діяльність" від 7 грудня 2000 р., затвердженого Постановою № 2121-III, встановлено, що інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та відносин з ним чи третіми особами при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту, є банківською таємницею. Порядок та межі розкриття банками інформації, що містить банківську таємницю, передбачений цим же законом. Так, відповідно до ст. 62 закону інформація щодо юридичних та фізичних осіб, яка містить банківську таємницю, розкривається банками, зокрема на письмовий запит або з письмового дозволу власника такої інформації. Такі положення даного закону остаточно та повно (поряд з положеннями Закону України "Про інформацію") узгоджують необхідність договірного врегулювання порядку розповсюдження інформації, яка стає відомою банку в межах обслуговування певного клієнта, якщо вона містить банківську таємницю.

Отже, в процесі обслуговування клієнтів установа має ґрунтовно проаналізувати перелік інформації, що створюється та підлягає розповсюдженню, та сегментувати її на загальнодоступну та конфіденційну. Адже законодавчі формулювання дають загальні визначення понять і дозволяють самостійне трактування економічними суб'єктами принципів відношення інформації до розряду тієї, що може завдати її власнику "матеріальної чи моральної шкоди". Так, статтею 30 Закону України "Про інформацію" передбачено самостійне визначення користувачем інформації порядку її розповсюдження та використання. Таким чином, банки зобов'язані

мати у своєму арсеналі низку внутрішніх нормативних документів, які регламентують принципи класифікації та правила використання інформації, що стає їм відомою в ході економічної діяльності.

У порядку відношення інформації до однієї із запропонованих класифікацій щодо обмежень доступу до неї банки враховують ряд факторів, що можуть спричинити певні наслідки розголошення інформації. До таких факторів слід відносити такі:

- репутаційні ризики, що виникають при розповсюдженні інформації;
- інформаційні ризики, що виникають внаслідок неузгодженості операційних систем та/або в результаті витоку інформації через технічний збій або через несанкціоновані зловмисні дії співробітників банку, що мають доступ до інформації;
- джерела отримання, спосіб використання та вимоги до умов зберігання інформації, що стає доступною банківським службовцям у ході виконання покладених на них обов'язків.

Інформаційні ризики входять до групи операційних ризиків і пов'язані з потенційними витратами, що можуть бути викликані неузгодженістю поточних процесів у ході банківської діяльності. Інформаційні ризики передусім пов'язують з розміщенням, зберіганням та обробкою інформації в автоматизованих системах установи. Об'єктом ризику в даному випадку є інформація, яка накопичується в різноманітних програмних комплексах банку. Інформація потрапляє в автоматизовану банківську систему на етапі започаткування правовідносин клієнта з установою, проте надалі ця інформація проходить численні етапи обробки та за ходом історії спільних відносин обростає новими відомостями. Будь-яка інформація про клієнта, яка вноситься в певну базу даних та містить персональні відомості про особу, вже вважається конфіденційною, оскільки згідно з умовами договору, незалежно від продукту чи послуги, передбачає обмежений доступ до цих даних.

У той же час інформаційний ризик виникає і як потенція виникнення помилок технічного, технологічного або персонального характеру внаслідок, наприклад, непрофесійних або недбалих дій працівників. Запобігання та упередження таких ризиків в установі вбачається досягти через детальне обстеження всіх напрямків і стадій роботи з інформацією та чітке узгоджене описання процедур і заходів інформаційної безпеки на кожному етапі. Здавалося б, координація роботи банківської установи з інформацією про клієнта вимагає дотримання певних практичних правил, приписаних чинними законодавчими актами. Алгоритм утримання такої конфіденційної інформації виглядає як фіксація видів таємної інформації в договорі з клієнтом, визначення в цьому договорі порядку використання такої інформації та надійне зберігання конфіденційної інформації в апаратних системах установи.

Утім, інформація по суті являє собою категорію, що значно ширша, ніж відомості для фундації разових відносин з клієнтами. Творче

багатофакторне використання інформації про клієнта, його ділову та побутову історію, обробка цих даних в аналітичних та статистичних комплексах дає банку місткий матеріал для примноження своїх прибутків. Саме на цьому етапі інформація набуває значно більшої цінності та стає привабливим ресурсом у контексті конкурентних відносин. Відтак створюється прецедент для появи репутаційних ризиків як потенційної неспроможності банку захистити інформацію про свої клієнтів всіма можливими технічними та технологічними засобами від поширення її за межами установи. Наслідки настання репутаційного ризику, спричиненого витоком інформації, можуть бути значно тяжчими, аніж результати виникнення технічного або технологічного ризику. Оскільки репутаційний ризик по суті має гіперболічно мультиплікаційний ефект популяризації негативної репутації про установу та, внаслідок своєї належності до системи зовнішніх ризиків, він має слабкий імунітет до небажаного розповсюдження в просторі та часі та, як наслідок, неминуче призводить до фінансових ризиків через неконтрольований відтік розчарованих клієнтів.

З метою запобігання настанню випадків, що можуть призвести до виникнення зазначених ризиків, державою започатковано основоположні заходи, яких банки мають дотримуватися щодо роботи з інформацією. Регламентні параметри таких заходів банки мають прописувати на рівні внутрішніх нормативних документів – це і формує систему інформаційної безпеки на макрорівні – проте структурне збереження класифікації заходів лишається непорушним для всіх фінансових установ. До заходів, що мають ретельно прописуватися в межах операційної діяльності банку, належать:

- класифікація інформації на загальнодоступну та конфіденційну (регламентовано ст. 30 Закону України “Про інформацію”);
- порядок обробки конфіденційної інформації та розкриття її як такої, що становить банківську таємницю (регламентовано гл. 10 (ст. 60–62) Закону України “Про банки і банківську діяльність”);
- ідентифікація клієнтів (регламентовано ст. 64 Закону України “Про банки і банківську діяльність”);
- зберігання документів, що містять конфіденційну інформацію (регламентовано ст. 65 Закону України “Про банки і банківську діяльність”);
- реєстрація баз даних, що містять конфіденційну інформацію (регламентовано ст. 31 Закону України “Про інформацію”), а також роботу з персональними даними (регламентовано Законом України “Про захист персональних даних” від 01.06.2010, який набирає чинності 01.01.2011).

Окресливши перелік процесів, які убезпечують роботу з інформацією на мікрорівні банківського інституту як суб’єкта економічних відносин, необхідно визначити практичний перелік даних, що становлять сам об’єкт захисту. Отже, пропонується розглядати роботу з інформацією з боку

банківських продуктів і послуг, які використовують або утворюють у ході свого життєвого циклу інформацію, що є об'єктом збереження.

Дистанційне банківське обслуговування є системою модернізованих банківських послуг, які надаються широкому колу клієнтів дистанційними каналами. Дистанціювання установи від особи, що запитує інформацію, суттєво ускладнює процес її ідентифікації, а отже, накладає обмеження щодо переліку даних, доступних для розголошення. Отже, при виведенні інформації на обслуговування дистанційним каналом процедура, що регулює її розповсюдження, вимагає ретельного обстеження та детального опису кожного окремого кроку комунікації установи з клієнтом.

З метою структурованого комплексного погляду на циркуляцію інформаційних потоків у системі дистанційного банківського обслуговування клієнтів пропонується класифікувати його на інформаційне та практичне. Інформаційне обслуговування полягає в наданні клієнтам загальнодоступної, в тому числі продуктової інформації, яка може бути розповсюджена відкритими каналами та надаватися у вільному доступі до неї. При цьому загальнодоступна інформація може надаватися без обмежень як діючим, так і потенційним клієнтам.

До загальнодоступної інформації належать відомості щодо ринкової діяльності банківської установи, її керівництва, мережі відділень установи, адреси, телефонні номери та інша контактна інформація. З переліку загальнодоступної продуктової інформації слід визначити відомості про номенклатуру пропозиції банківського продуктового ряду, послуги відносно цих продуктів та умови їх надання, тарифи на відкриття та обслуговування. Загальнодоступна інформація розповсюджується та доводиться до клієнтів незахищеними інформаційними каналами та не передбачає ідентифікації клієнта при його оповіщенні.

У контексті різновидів банківського обслуговування, а саме традиційного чи дистанційного обслуговування, немає жодної різниці щодо порядку розголошення загальнодоступної інформації – чи то відомості публікуються на інформаційних дошках у відділенні установи, чи то відображаються на веб-сторінках корпоративних Інтернет-сайтів, чи то надаються у вигляді консультації у відділенні чи по телефону.

Конфіденційна інформація, визначена на рівні внутрішньобанківських процедур, інформація, що, згідно з законодавством, містить банківську таємницю, а також інформація персонального характеру привносить суттєві обмеження щодо порядку її акумуляції, супроводження та розголошення. Недарма інформацію, стосовно якої застосовується обмежений режим доступу, ми розподілили на три види, адже регулювання роботи з кожним з них запроваджено різними документами чинного законодавства або в багатьох випадках внутрішніми процедурними регламентами. Проте аби надати концептуальний підхід до роботи з такою інформацією, припустимо її ідентичність та визначимо як інформацію з обмеженим доступом.

Інформація з обмеженим доступом (надалі в цьому блоці – Інформація) характеризується низкою вимог при опроцесуванні, а саме:

1. Опрацювання та формалізація порядку роботи на внутрішньому рівні по кожному з об’єктів Інформації, що передбачає розробку нормативних документів щодо видів такої інформації, її ознак, правил збереження та адміністрування, а також умови, за яких відомості може бути розголошено.
2. Обмеження та порядок доступу до Інформації персоналу згідно з фактичними ролями при роботі з Інформацією, що передбачає визначення осіб, уповноважених до роботи з інформацією, а також меж та умов користування нею.
3. Специфіка, передусім обмеження, і порядок розповсюдження Інформації дистанційними каналами, що передбачає визначення ознак Інформації з різними межами доступів, а також вибір параметрів ідентифікації права особи на отримання даних.
4. Системи сховища Інформації та порядок передавання даних за межі установи, засоби шифрування та безпека каналів передавання, що передбачає визначення технічних вимог щодо апаратно-технологічної платформи та правил настройки програмних засобів для захищеного розповсюдження відомостей.

Надзвичайно важливим аспектом у контексті роботи банківських установ з інформацією, зокрема й у системі дистанційного обслуговування, є державна політика, що реалізується через певні норми законодавства та через контрольно-ревізійну діяльність регуляторних органів. Основним завдання держави в цьому напрямку є створення сприятливого та безпечного клімату для ринкової діяльності учасників галузі за умови дотримання останніми адекватної державній політиці системи роботи з інформацією.

Суттєві ускладнення в ході спільних заходів законодавчих інститутів і банківських установ як економічних суб’єктів ринку щодо роботи з інформацією викликає низка нормативних положень, формалізація яких на законодавчому рівні не відповідає практичному підґрунтю для реалізації відповідних вимог. В арсеналі національних нормативних актів є теоретичні тлумачення норм, які фактично не можуть бути виконані економічними суб’єктами внаслідок незавершеної або непідготовленої організаційно-технологічної бази з боку держави.

Найсвіжіший документ, що стурбував коло гравців ринку фінансових послуг, – Закон України “Про захист персональних даних”, прийнятий 1 червня поточного року (надалі в цьому блоці – Закон). Дискусії навколо положень Закону поглиблюють наближення дати введення його в дію з початку наступного року. Насамперед слід зауважити, що термінологічний блок Закону не висвітлює низки понять, про які йдеться в документі. Так не надано визначення поняття, процесу та параметрів проведення ідентифікації, з якою пов’язано ряд напрямків роботи з персональними даними. Трактування персональних даних як відомостей, за якими особу може бути ідентифіковано, є неповним, оскільки принципи ідентифікації не встановлено. Розпливчастим є формулювання ознак третьої особи як суб’єкта відносин по використанню

персональних даних, оскільки тісно перетинається з визначенням альтернативного розпорядника даних. Проголошені вимоги Закону щодо роботи з персональними даними в деяких напрямках докорінно деформують встановлені процедури інформаційної діяльності банків. Так, наприклад, статтею 2 Закону установам дозволено обробляти дані про своїх клієнтів лише на підставі письмового дозволу на обробку – зауважимо, що договірні угоди між банками та клієнтами при розголошенні останніми своїх персональних даних сформульовано на вимогу ст. 64 Закону України "Про банки і банківську діяльність", якою на банки покладено обов'язок ідентифікації клієнта при укладанні з ним фінансових відносин. При цьому з посиланням на вимоги Закону "Про захист персональних даних" банки позбавлені можливості здійснювати стосовно клієнта маркетингові та інші ініціативні активності, якщо така мета обробки персональних даних клієнта не визначена в договорі.

Доцільно було б провести паралель роботи з персональними даними на мікрорівні банківської установи, де зобов'язані законодавчими вимогами суб'єкти вже давно чітко прописали принцип однозначної ідентифікації особи за унікальними даними, документально підтвердженими при укладанні економічних відносин. З тим можна стверджувати, що банківські нормативні документи зробили значний крок уперед у контексті формалізації інформаційної діяльності стосовно своїх клієнтів та сформували стійку платформу для розвитку дистанційного напрямку обслуговування.

Низка колізійних положень присутня також у Законі України "Про інформацію", а саме ст. 31 установи, що збирає інформацію про громадян, зобов'язано провести державну реєстрацію баз даних у порядку, визначеному Кабінетом Міністрів. Зауважимо, що порядку такої реєстрації та навіть органу при Кабінеті Міністрів, який зорганізовано для забезпечення подібної функції, наразі не існує. Посилання на органи державної влади уповноважені здійснювати наглядову та контролюючу функцію стосовно установ, які працюють з персональними даними, до яких значною мірою належать банки, також зафіксовано в ст. 4 Закону України "Про захист персональних даних".

Вимоги щодо організаційних заходів з боку установ при роботі з персональними даними, визначеними ст. 6 цього ж Закону, значно ускладнює гнучкість інформативного впливу банків на своїх клієнтів насамперед у межах прогресивного дистанційного обслуговування та провокує чисельні непродуктивні контакти з власником даних з приводу розширення спектра використання інформації установою. Економічна ефективність від такої холостої взаємодії банку з клієнтом, породженої бюрократизованим алгоритмом так званого убезпечення інформації, стрімко знижується.

Також суперечливі неузгоджені положення чинних законодавчих актів викликають ускладнення та унеможливлюють інформаційну, в тому числі маркетингову діяльність банківських установ. Наприклад, ст. 23 Закону України "Про інформацію" визначено поняття "інформації про особу", яке в тому числі включає персональні дані про особу. Відомості, що належать до

персональних даних, чітко визначено положеннями даної статті. Статтями 28, 30 та 31 цього ж закону визначено дозвіл на узгоджений між власником інформації та розпорядником (у нашому випадку банком) у письмовій формі порядок використання таких даних. У той же час ст. 7 наразі впровадженого Закону України "Про захист персональних даних" перелічено відомості про особу, обробка яких є забороненою. У тій же статті перелічені випадки скасування заборони на роботу з відповідними видами даних, проте жоден з них не має економічного характеру використання.

Висновки. Ключовим моментом у всіх процесах дистанційного обслуговування Інформації є принципи ідентифікації клієнта та його прав на отримання певної інформації. У чинних нормативно-правових актах чітко визначено необхідність проведення ідентифікації клієнта при розголошенні йому інформації, що містить банківську таємницю. При цьому порядок такої ідентифікації має бути розроблений банком самостійно та впроваджений на технологічному та організаційному рівнях у виробничу експлуатацію. У межах легалізації процесів роботи з Інформацією при дистанційному обслуговуванні та з посиланням на окреслену концепцію політики установи щодо інформаційно-практичного обслуговування банкам рекомендується запроваджувати комплекс таких заходів:

1. Визначення принципів аутентифікації працівників, які отримують доступ до Інформації: порядок урізання прав до різних сегментів Інформації, періодичність корекції таких прав, правила моніторингу і контролю доступів.
2. Встановлення параметрів ідентифікації клієнтів по всіх продуктах, які передбачають надання Інформації дистанційним каналом.
3. Визначення каналів розповсюдження Інформації з набору дистанційних каналів та їх сегментація для розробки різних підходів до убезпечення (Інтернет-канал, телефонний зв'язок, IVR-ресурс).
4. Визначення та прогноз ризиків, що супроводжують процеси оприлюднення інформації дистанційним каналом.
5. Узгодження методології бізнес-процесу розповсюдження Інформації дистанційним каналом та визначення показників моніторингу.
6. Дослідження та вибір постачальника та інтегратора програмних рішень, що супроводжують процеси адміністрування Інформацією.
7. Визначення політики інформаційної безпеки щодо передавання Інформації каналами зв'язку, розробка та реалізація підходів до шифрування та дешифрування інформації.

Слід зазначити, що дослідження та вирішення наведених вище завдань є тривалою та кропіткою роботою згуртованої команди банківських фахівців. При цьому коректна та ефективна реалізація згаданих опцій передбачає узгоджену взаємодію підрозділів банківського бізнесу (продуктові ланки та представники підрозділів продажу), фахівців з інформаційних технологій, в тому числі комп'ютерної та інформаційної безпеки, юридичних служб та підрозділів ризик-менеджменту.

Побудова бізнес-процесу виведення чергового банківського продукту на альтернативний дистанційний канал обслуговування на сьогоднішній день є звичним завданням продуктових менеджерів банку. Адже сучасний клієнт вимагає оптимізації процесів продажу та обслуговування продуктів, а конкуренти не припиняють свою діяльність у галузі технологізації послуг. Втім, методика та комплекс заходів захисту інформації, що має цінність для установи, в цілому зберігається по всіх установах.

Слід відмітити, що персональні дані особи є цінним матеріалом для продуктової та маркетингової активності фінансової установи, яка переважно здійснюється саме в межах дистанційного обслуговування. За допомогою набору відомостей про особу, яка є або потенційно може стати клієнтом, банки готують продуктову пропозицію, здійснюють продаж та вдосконалюють програми обслуговування, найбільш вдалі для конкретного клієнта. Дослідницька та маркетингова діяльність банків, яка передусім пов'язана з обробкою великих масивів інформаційних даних, насамперед персональних, створює презентативний матеріал для визначення економічної зрілості споживача, його вподобань, виховання лояльності та, як наслідок, оптимізує відносини між суб'єктами ринку.

Отже, інтегрована діяльність банківських інституцій з представниками законотворчої державної ланки, об'єднання ідей теоретичної активності владних структур та адаптація їх практичних ринкових потреб є на сьогоднішній день актуальною роботою в межах створення вільно-прогресивного суспільно-економічного простору.

Список літератури

1. Диба, М. Інформаційні ризики в банківській діяльності [Текст] / М. Диба, М. Зубок, С. Яременко // Вісник Національного банку України. – 2007. – № 9. – С. 28–36.
2. Кормич, Б. А. Інформаційна безпека: організаційно-правові основи [Текст] : навч. посібник / Б. А. Кормич. – К. : Кондор, 2004. – 384 с.
3. Малюк, А. А. Інформаційна безпека: методологічні й концептуальні основи захисту інформації [Текст] А. А. Малюк // М. : Гаряча лінія-Телеком, 2004. – С. 280.
4. Примостка, Л. О. Управління банківськими ризиками [Текст] : навчальний посібник / Л. О. Примостка. – КНЕУ, 2007. – 539 с.
5. Про банки і банківську діяльність [Текст] : Закон України // Відомості Верховної Ради України. – 2001. – № 5–6. – 30 с.
6. Про захист персональних даних [Текст] : Закон України від 2 червня 2010 року № 2297-V. – Режим доступу : http://www.president.gov.ua/documents/ 11965.html.
7. Про інформацію [Текст] : Закон України від 2 жовтня 1992 року // Відомості Верховної Ради України. – 1992. – № 48 [зі змінами від 06.04.2000] // Відомості Верховної Ради. – 2000. – № 20.
8. Снытников, А. А. Обеспечение и защита права на информацию [Текст] А. А. Снытников, Л. В. Туманова. – М. : Городец-издат, 2001. – 344 с.

Summary

Remote services being a part of progressive banking is requested for modern adjusted implementation approach. Bank info in terms of it remote service background needs to be secured on the level of legal, technology and operations. Research dedicates to multifactor data security for bank risks minimizing.

Отримано 15.12.2010

Шалига, Т.С. Регулювання порядку роботи з інформацією при банківському дистанційному обслуговуванні / Т.С. Шалига // Проблеми і перспективи розвитку банківської системи України: зб. наук. праць.- Суми: УАБС НБУ, 2010.- Т. 30.- С. 316-328.