УДК 346:[004.78:336.717]

Підболячний В. Ф.

ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БАНКІВСЬКІЙ СФЕРІ

In the article the problems of organizational-legal support of information safety in a banking sector are considered. The comparative analysis of Ukraine legal support situation is reduced. Besides, the main ways of implementation of state information safety conceptual positions on the basis of normative-legal and organizational regulating of the given sphere are offered.

Питання забезпечення інформаційної безпеки сьогодні для України знаходяться на одному рівні із захистом суверенітету й територіальної цілісності, її економічних та інших першочергових життєво важливих інтересів. Інформаційна безпека, головні проблеми організації якої є предметом розгляду, співвідноситься з національною безпекою як частина і ціле. Ці поняття взаємопов'язані: як інформаційна безпека не може існувати поза межами національної безпеки, так і національна безпека не буде всеохоплюючою у разі позбавлення її інформаційних векторів.

Прийнятий Верховною Радою України Закон України "Про основні заходи розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" [1] передбачає постійне вдосконалення необхідних для цього правових норм та інститутів. Без сумніву, нормативно-правове регулювання є базовим інструментом захисту національної безпеки в цілому та інформаційної безпеки як її складової, в тому числі у фінансово-банківській сфері.

Метою статті є показ існуючого стану організаційно-правового забезпечення інформаційної безпеки в банківській сфері.

За декілька останніх десятиріч вимоги до інформаційної безпеки істотно змінювалися. До початку широкого використання комп'ютерних систем безпека інформації досягалася виключно фізичними й адміністративними заходами. З появою комп'ютерів стала очевидною необхідність використання програмних засобів захисту файлів даних і програмного забезпечення. Наступний етап розвитку програмних засобів пов'язаний з появою розподілених систем опрацювання даних і комп'ютерних мереж передачі даних.

Необхідність захисту бізнесу самим бізнесом у будь-якій країні є явищем об'єктивним [2]. І однією з основних умов існування та ефективності такого захисту є нормативно-правові заходи, які розробляє держава. У цивілізованих країнах світу цей захист здійснюється на приватному рівні, тобто без втручання державних інстанцій, у 70% випадків. Як же виглядає це питання у використанні до такого виду досить розвинутого в нашій державі бізнесу, як забезпечення безпеки банківської діяльності?

Певна система, безумовно, є. Але необхідно зазначити, що спеціального законодавства в цій галузі на сьогодні немає, є тільки окремі положення законодавчих та нормативних актів [3].

Сприймаючи безпеку банківської діяльності як багатогранну систему захисту інтересів банку, можливо позначити її основні види, під якими розуміють сукупність заходів єдиної спрямованості. Сьогодні це:

особиста безпека;

колективна безпека;

економічна безпека;

інформаційна безпека, під якою мається на увазі формування інформаційних ресурсів банку та організація гарантованого їх захисту. Досягається створенням системи збору та обробки інформації проведенням відповідних заходів щодо її зберігання та розподілу, визначення категорій і статусу, порядку і правил доступу до неї, дотримання усіма працівниками, клієнтами, контрагентами та акціонерами банку норм і правил роботи з банківською інформацією, своєчасним виявленням спроб і можливих каналів витоку інформації та їх припиненням й перекриттям.

Однак, для сучасного банку питання забезпечення інформаційної безпеки є дійсно важливим. Це підтверджується такими положеннями.

По-перше, сьогоднішня банківська установа з погляду інформаційної безпеки є компанією "підвищеного ризику". Банк – це зосередження грошей, цінних документів, збережень, металів. При цьому автоматизована банківська система, невід'ємна складова корпоративної інформаційної системи банку, підтримує процеси проведення виплат, надання кредитів, обслуговування депозитів, переказ коштів та ін. Вона є основою функціонування практично всіх бізнес-процесів, й, очевидно, незаконне маніпулювання такою інформацією може призвести до серйозних збитків.

По-друге, сучасний банк надає велику кількість сервісів, пов'язаних з віддаленим доступом до інформаційної системи банку. Це й персональний Інтернет-банкінг, і система Інтернет-доступу до фінансових ринків, і система електронного документообігу та багато іншого. Із цих позицій банк – точка перетину публічних мереж (Інтернету) і комерційних фінансових мереж (Visa Net [4], Swift [5] та ін.).

По-третє, на сьогоднішній день банки мають складні інформаційні системи, які включають великий набір "бек-офісних" і "фронт-офісних" застосувань. А управління цими системами ускладнюється через територіальну розпорошеність підрозділів банків, наявність чисельних філій, офісів та відділень (в Україні є близько десятка комерційних банків, кількість територіальних підрозділів яких (так званих відділень) нараховує понад 500, а в 2 – 3 – понад 1 000).

По-четверте, банк зберігає персональні дані громадян й конфіденційну інформацію своїх клієнтів – і юридичних, і фізичних осіб. Останнє є дуже "чутливою" обставиною й на практиці все частіше стає предметом серйозних конфліктів, включаючи кримінально-процесуальні рамки.

Вищевказані фактори висувають жорсткі вимоги до захисту корпоративної інформаційної системи сучасного банку, основними з яких є:

комплексність;

інтегрованість;

адекватність затратам;

легітимність;

керованість;

масштабованість;

відмовостійкість.

Утім, цей перелік вимог є далеко не вичерпаним. Можна виділити такі базові вимоги до корпоративної мережі банку:

а) поєднання у структуровану замкнену систему всіх інформаційних пристроїв, що належать банку: окремі комп'ютери і локальні мережі, сервери, робочі станції, телефони, факси, офісні АТС, мережі банкоматів, онлайнові термінали;

б) забезпечення надійності функціонування та дієвості систем захисту інформації;

в) гарантованість безвідмовної роботи системи як при помилках персоналу, так і у випадках спроби несанкціонованого доступу;

г) забезпечення налагодженого зв'язку між банківськими відділеннями різного рівня на всій території держави, а для іноземних банків – і міждержавного зв'язку;

д) забезпечення цілодобового доступу до банкоматів та онлайнових терміналів, можливості цілодобових операцій з рахунками клієнтів;

е) організація оперативного, надійного і безпечного доступу віддаленого клієнта до сучасних банківських послуг.

З боку органів регулювання до банку також висувається ряд вимог та пропонується комплекс рекомендацій [6] із забезпечення інформаційної безпеки. Це постанови й інструкції НБУ, міжнародні стандарти, вимоги Basel II [7], різні вимоги міжнародних платіжних систем та ін.

Наведемо короткий огляд найбільш складних загроз і основних проблем інформаційної безпеки банку.

Серйозною загрозою сьогодні є небезпека ураження комп'ютерними вірусами і різними деструктивними програмами, що несе за собою величезні фінансові збитки. За результатами досліджень, проведених компанією InformationWeek Research [8], у 2008 році орієнтована сума втрат, заподіяних вірусами та хакерськими атаками, склала близько 1,9 трлн дол. Тут головним завданням для відповідних служб банку є створення і втілення комплексного антивірусного захисту з метою недопущення зараження або швидкого "виліковування" комп'ютерної системи. Цим вимогам відповідає переважна більшість продуктів сучасного ринку, потрібно тільки визначитися в особливостях для кожного випадку.

Ще один з найбільш небезпечних сьогодні для банків видів загроз – несанкціонований доступ. Такого роду інциденти мають щорічно більша частина діючих в Україні банківських установ. Відповідно все це призводить до величезних втрат. Для вирішення завдань захисту від такого доступу використовується цілий комплекс заходів: технічні, програмно-апаратні, адміністративно-правові, організаційні. Побудові ефективного захисту системи повинен передувати професійно грамотний попередній аналіз можливих загроз, який має містити:

оцінку цінності інформації, що є в системі;

оцінку витрат часу й засобів для подолання захисного бар'єру;

оцінку характеру інформації, що зберігається, виділення імовірних найнебезпечніших способів загроз;

оцінку витрат часу, засобів і ресурсів системи захисту;

побудову моделі особи зловмисника.

Щодо останнього – хакер по відношенню до системи, яку він атакує, може виступати в ролі (по наростаючій):

сторонньої особи, яка використовує загальнодоступну глобальну мережу;

співробітника банку, який не має легального доступу до даної системи;

користувача системи, який володіє мінімальними повноваженнями;

адміністратора системи;

розробника системи.

Проблема обтяжується ще й тим, що для несанкціонованого доступу часто потрібна крадіжка конфіденційної інформації. У результаті такої комбінації двох надзвичайно небезпечних загроз збитки можуть зрости в декілька разів.

Дослідження показують, що безпосередній несанкціонований доступ до електронно-обчислювальних машин [9], систем та комунікаційних мереж робиться, в основному, співробітниками банків: програмістами, інженерами, операторами, які є користувачами або обслуговуючим персоналом – 41,9%. Майже вдвічі – інші співробітники банку – 20,2%, а в 8,6% випадків злочин вчинено співробітниками, яких звільнено, і лише 25,5%, коли несанкціонований доступ вчинений сторонньою особою.

Що стосується банків, які постраждали, то їх службовці не дуже зацікавлені в реєстрації таких злочинів і нерідко це приховують. Адже розголошення факту здійснення злочинних дій проти комп'ютерної системи банку негативно відобразиться на авторитеті установи та призведе до можливої втрати клієнтів. А ось внутрішні розслідування проводяться практично завжди.

Зростання номенклатури банківських послуг із використанням Інтернету для фізичних і юридичних осіб, особливо пов'язаних з управлінням рухом коштів на рахунках системи дистанційного банківського обслуговування, призвели до появи загроз, які потенційно несуть ризик прямої втрати коштів – атак з мережі Інтернет на ресурси банку з метою неправомірного отримання персональної інформації користувачів систем дистанційного банківського обслуговування. Такі атаки мають назву "фішингових". За даними Anti-Phishing Working Group [10] 92 – 94% усіх таких атак мали місце саме по відношенню до фінансового сектору. При здійсненні фішингових атак користувачам систем дистанційного банківського обслуговування електронною поштою направляються повідомлення, якими під різними приводами пропонується ввести певні дані в поле екранних форм у ході сеансів імітованої інформаційної взаємодії з банком (наприклад, через створений дублікат цього веб-сайта). Одночасно на комп'ютері клієнта з підробленого веб-сайта можуть передаватися шкідливі програми, які виконують приховані функції, пов'язані з неправомірним отриманням персональної інформації користувача, такої як паролі, PIN-коди, криптографічні ключі, номери банківських карт тощо. У подальшому, з використанням отриманих таким чином даних, шахраї здійснюють крадіжки з рахунку жертви.

В Україні й країнах пострадянського простору статистики щодо фінансових збитків від фішингу немає. У 2008 році зареєстровано низку (декілька десятків) фінансових атак на деякі українські банки і операторів мобільного зв'язку. За оцінками фахівців, результативними з них є не більше 10%, тобто більшість таких атак не проходять через виставлені підрозділами інформаційної безпеки бар'єри.

Тут доречно декілька слів сказати про сьогоднішню комп'ютерну злочинність в Україні. Рівень криміналізації інформаційно-телекомунікаційної сфери зростає високими темпами. Так, якщо у 2003 – 2004 роках органами СБУ України було порушено 7 кримінальних справ у сфері протиправного застосування інформаційно-телекомунікаційних технологій, то вже в 2005 році їх кількість зросла до 40. Приблизно така ж ситуація мала місце і в наступні роки. І найхарактернішими для цього періоду протиправними діями є несанкціоноване втручання в роботу автоматизованих систем, створення та розповсюдження комп'ютерних вірусів, несанкціонований збут інформації з обмеженим доступом.

У той же час проведений фахівцями СБУ аналіз сучасної ситуації у сфері забезпечення інформаційної безпеки свідчить про суттєве відставання України від системних заходів, у першу чергу, правового характеру, що вживаються провідними державами світу.

Так, на ефективність діяльності правоохоронних органів у напрямку забезпечення інформаційної безпеки негативно впливає недосконала нормативно-правова база у сфері протидії комп'ютерній злочинності. Незважаючи на те, що Верховною Радою України ратифіковано Міжнародну конвенцію про кібер-злочинність [11], є ціла маса проблемних правових питань, невирішеність яких стримує ефективну реалізацію правозастосовних функцій не тільки Служби безпеки, а й інших державних і недержавних інституцій, що протидіють комп'ютерній злочинності та комп'ютерному тероризму. Ось основні з них.

Сьогодні не вирішено проблему законодавчого регулювання правових відносин між суб'єктами ринку Інтернет-послуг, зокрема відсутнє відповідне нормативно-правове регулювання підприємницької, в тому числі банківської діяльності з надання послуг доступу до мережі Інтернет [12].

У зв'язку з ратифікацією вже згаданої Конвенції про кіберзлочинність уже зараз потрібно вносити певні зміни до Кримінального та Кримінально-процесуального кодексів України відповідно до вимог міжнародного законодавства, адже наявний вміст розділу XVI КК України [9] не враховує міжнародного підходу до визначення кола суспільно небезпечних діянь, що визнаються комп'ютерними правопорушеннями щодо інформації, а саме: незаконний доступ; нелегальне перехоплення; втручання у дані; втручання у систему; зловживання пристроями; підробка, пов'язана з комп'ютерами; шахрайство, пов'язане з комп'ютерами та ін. Узагалі, чинний Кримінальний Кодекс України містить цілу низку складів злочинів, які можуть бути віднесені до категорії інформаційних, але розміщені в різних розділах Кодексу, що зумовлює визначення родових об'єктів цих злочинів різними. Тобто, на думку фахівців, враховуючи сучасний рівень розвитку інформаційних відносин та зростаючу значущість інформаційних ресурсів, доцільно виділити в окрему групу інформаційні злочини, родовим об'єктом яких є суспільні відносини у сфері інформаційної безпеки (такі, як забезпечення безпеки інформації, безпеки від впливу інформацією та захисту прав суб'єктів інформаційних відносин), тобто створити окремий розділ Кримінального Кодексу України – "Злочини у сфері інформаційної безпеки".

Є багато інших проблем правової неврегульованості, але дещо й робиться.

Опрацьовуються відповідні законопроекти. Підписано Конвенцію про захист осіб стосовно автоматизованої обробки персональних даних та додатковий протокол до неї [13].

Останнім часом відбулася досить серйозна трансформація інформаційної організації держави. Організаційно-правові засади у сфері інформаційної безпеки, що діють сьогодні в Україні, загалом створюють необхідні передумови для реорганізації відповідної державної політики. Проте новий витік технологічних успіхів в інформатиці поряд із прогресивними можливостями, що відкриваються, породжує й нові загрози безпеці. Сьогодні в Україні діє декілька десятків нормативно-правових актів, що регулюють цю галузь [14].

Основні шляхи реалізації концептуальних положень інформаційної безпеки держави мають бути визначені в науково-обґрунтованій доктрині інформаційної безпеки, прийняття якої очікується. Ця доктрина повинна бути продовженням Стратегії нацбезпеки та має розроблятися законодавчими органами й керівництвом держави, а її основні вимоги повинні бути деталізованими в законах держави й інших нормативно-правових актах, а також у вигляді цільових державних програм і проектів.

Доводиться констатувати, що процес інформатизації має сьогодні в Україні стихійний, некерований характер, з переважним ухилом у бік використання засобів інформатизації іноземного виробництва. Безсистемність процесів формування інформаційної структури в Україні обумовлює складнощі вирішення проблем інформаційної безпеки, захисту інформаційних ресурсів.

У цілому ж можна зробити узагальнюючий висновок про те, що основним питанням забезпечення інформаційної безпеки на сьогодні є необхідність нормативно-правового й організаційного регулювання цієї галузі. Тому пріоритетним завданням є подальше створення й удосконалення законодавчої та нормативно-правової баз. Зокрема, йдеться про необхідність прийняття Закону "Про інформаційну безпеку", який би регулював суспільні відносини у цій сфері. Цей закон, спроба прийняття якого, як відомо, вже була в 2005 році, окреслив би засади для формування державної політики інформаційної безпеки, розвитку інформаційного простору країни.

Існує також необхідність у створенні координаційної комісії з питань нормативно-правового забезпечення інформаційної безпеки, яка б стала акумулятором пропозицій різних органів державної влади, недержавних структур, громадських організацій у цій справі.

Підсумовуючи проведене дослідження, можна окреслити коло загальнодержавних заходів, вжиття яких є нагальним та сприятиме підвищенню рівня нормативно-правового забезпечення інформаційної безпеки держави. Ось основні з них:

прийняття законів України "Про інформаційну безпеку", "Про захист персональних даних", "Про перехоплення телекомунікацій";

ратифікація Верховною Радою України Конвенції про захист осіб стосовно автоматизованої обробки персональних даних;

запровадження ліцензування господарської діяльності у сфері надання доступу до мережі Інтернет провайдерами таких послуг та утримувачами пунктів колективного доступу до Інтернет із визначенням умов організації такого доступу відповідно до вимог Конвенції про кіберзлочинність [11];

створення координаційної комісії з питань нормативно-правового забезпечення інформаційної безпеки;

відновлення роботи міжвідомчої групи з розробки Державної програми з протидії комп'ютерній злочинності;

активізація роботи з приведення чинного законодавства у відповідність до встановлених міжнародних стандартів та норм.

Проведено аналіз проблем правового й організаційного регулювання інформаційної безпеки безпосередньо в банківській сфері. Інформаційні взаємовідносини суб'єктів підприємництва і держави регулюються сьогодні понад 30-ма законодавчими і майже такою ж кількістю підзаконних актів. Інформаційна банківська безпека знаходиться на стику трьох правових полів: суто інформаційного, банківського і законодавства про права особи. Саме це зумовлює необхідність створення якогось більш визначеного кола "правил гри". Ураховуючи ж особливість діяльності банків у сфері економічних відносин як суб'єктів, що "зв'язують" функціонування всіх підприємств, організацій і установ через грошові потоки і взаєморозрахунки, а також велику кількість приватних осіб, виникає потреба в регулюванні їх суміжних інтересів щодо захисту інформації. Тобто, сьогодні в державі є потреба в публічному праві, яке б виступало механізмом державного регулювання і захисту інтересів суб'єктів підприємництва на ринку інформації. Можна констатувати, що існуюча сьогодні сукупність правових норм у сфері інформації та комп'ютеризації досягла за кількісними показниками такої критичної маси, що зумовлює можливість і реальну необхідність виділення, систематизації та кодифікації їх в окрему правову інституцію з подальшими стратегічно спланованими кроками із законодавчого та нормативно-відомчого удосконалення.

Структури із захисту інформаційної безпеки сьогодні в банках України є практично всюди, але діють вони розрізнено, автономно вирішуючи практично однакові проблеми. Певні спроби якось об'єднати свої зусилля в цьому напрямку в українській банківській історії були, але суттєвих успіхів вони не мали, тому що організовувались не системно, а за ініціативою окремих банків і окремих ентузіастів. Є декілька відомих українських банків, де рівень інформаційної безпеки дійсно розвинутий, високий і сучасний, наскільки це дозволяє правове поле, матеріально-фінансові можливості й кадровий потенціал. Вони й могли б під егідою і за ініціативою НБУ створити робочу групу для комплексної оцінки нинішнього стану банківської інформаційної безпеки і розробити конкретний механізм удосконалення цієї діяльності, без перебільшення дуже актуальної сьогодні, який би мав складатися з двох частин: законодавчий рівень та відомчі й міжбанківські питання. А наявність в Україні сьогодні декількох могутніх іноземних банківських установ, які працюють у нашому фінансовому просторі, дуже допомогли б цій справі, зробивши реальний внесок у структуру банківської безпеки.

На завершення хотілось би підкреслити, що інвестиції в інформаційну безпеку − це інвестиції в майбутнє. Там, де є такий підхід, сповідуються такі принципи:

1. Відповідність цілей, політик і процедур інформаційної безпеки цілям бізнесу.

2. Підтримка і зацікавленість станом інформаційної безпеки з боку керівництва банківської установи.

3. Чітке розуміння вимог безпеки, оцінка ризиків і керування ризиками.

4. Усвідомлення необхідності застосування заходів інформаційної безпеки всіма співробітниками, забезпечення їх підготовки і навчання.

Така стратегія управління інформаційною безпекою, відношення до неї дозволяє досягти головної мети для банківської установи − уникнення прямих та непрямих фінансових втрат, які є наслідками або пов'язані з інцидентами в інформаційно-телекомунікаційній сфері.

Література: 1. Закон України "Про основні заходи розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 9 січня 2007 року // Відомості Верховної Ради України. – 2007. – № 1–2. 2. Кавун С. В. Информационная безопасность в бизнесе : монография / С. В. Кавун. – Харьков : Изд. ХНЭУ, 2007. – 408 с. 3. Сайт Національного банку України [Електронний ресурс]. – Режим доступу: http://www.bank.gov.ua/B_zakon/index.htm. 4. Сайт системи Visa Net в Європі [Електронний ресурс]. – Режим доступу: http://www.visaeurope.com/. 5. Сайт системи SWIFT (Society for Worldwide Interbank Financial Telecommunication) [Електронний ресурс]. – Режим доступу: http://www.swift.com/. 6. Постанова Верховної Ради України "Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні" від 1 грудня 2009 року // Відомості Верховної Ради України. – 2006. – № 15. 7. Базельский комитет по банковскому