групи, результати якого ми оприлюднимо у наступних номерах журналу.

1. Тимошенко З.І. Соціально-політичні аспекти та перспективи участі України в Болонському процесі / З.І. Тимошенко // Матеріали міжнар. наук.-практ. конф. "Україна – суб'єкт європейського освітнього простору". – К.: Вид. Європ. ун-ту, 2005. – С. 9.

2. Сенашенко В., Ткач Г. Болонский процесс и качество образования // http://library.uipa.kharkov.ua/library/Documents/BolonProz/3/3_2.htm

3. Байденко В.И. Болонский процесс: структура реформ высшего образования Европы / В.И. Байденко. – М. : Исслед. центр проблем качества подготовки специалистов; Российский новый ун-т, 2002. – 1287 с.

4. The European higher education Area. Joint Declaration of the European Ministers of Education. Convened in Bologna on the 19th of June 1999 // http://www.bolognadec.html.

5. Towards the European Higher Education: Communiqué of the meeting of European Ministers in charge of Higher Education in Prague, 19 May 2001.

6. Shaping the European Higher Education Area: Message from the Convention of European Higher Education Institutions, Salamanca 25 – 26.03.2001 // News of the Recognition Field: Background Information for the ACE Track, 13th Annual Conference of the European Association for International Education (EAIE) 5 to 8 December, 2001, Tampere, Finland. – Riga: EAIE, Latvian ENIC/NARIC, 2001. – P. 51 – 52.

7. Realizing the European Higher Education Area: Communiqué of the Conference of Ministers responsible for Higher Education in Berlin on 19 September 2003.

8. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти. – К.: Ленвіт, 2006. – 35 с.

Стаття надійшла до редакції 07.09.2011

УДК 336.741.242

Валентина Страхарчук, *кандидат економічних наук,*
доцент кафедри економічної кібернетики
Анатолій Страхарчук, *кандидат економічних наук,*
професор кафедри комп'ютерних технологій
Львівського інституту банківської справи УБС НБУ

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЕЛЕКТРОННОГО БАНКІВСЬКОГО БІЗНЕСУ

Розглянуто та систематизовано гальмівні чинники розвитку електронного банківського бізнесу, проаналізовано світові стандарти критеріїв оцінки безпеки інформаційних систем, обгрунтовано та систематизовано основні недоліки криптографії, що базується на симетричних ключах. Визначено можливі варіанти підвищення ефективності функціонування електронного банкінгу.

Ключові слова: *електронний бізнес, ефективність електронного бізнесу, електронні банківські послуги, кібер-безпека, кібер-атака, кібер-злам, інформаційний захист.*

Рис. 2. Літ. 9.

Постановка проблеми. Сьогодні мережа Internet є інформаційною системою для оперативного здійснення банківських операцій. Відкритість мережі Internet для платежів і використання її як каналу збуту викликає у користувачів різного роду занепокоєність щодо безпеки здійснюваних фінансових операцій. Щоденно в світі здійснюються перекази на суму понад $ 4000 млрд з використанням електронних систем зв'язку. За даними Бюро технологічної оцінки США 0,1 – 0,15 % усіх переказів відносяться до відмивання "брудних" коштів. Річні збитки від шахрайських дій з пластиковими картками складають понад 1% від загального грошового обігу – близько 2,5 мільярдів доларів США [9].

Як свідчать дослідження, сьогодні існує ціла низка гальмівних чинників, що супроводжують процес надання електронних фінансових послуг в світі, і в Україні, зокрема, стримуючи розвиток відповідних інформаційних технологій, а, відтак, ефективного процесу надання електронних банківських послуг. Серед них чи ненайважливішим є ризикованість електронного бізнесу внаслідок недостатнього рівня безпеки. Відсутність сьогодні ефективних процедур забезпечення належного рівня кібер-безпеки, а, відтак, мінімізації ризикованості сфери електронного бізнесу, є стримуючим фактором розвитку фінансових кібер-технологій.

Світова фінансова криза сьогодні спонукає банки України, шукати безризикові технології обслуговування клієнтів, щоб захистити свій капітал, повернути довіру клієнтів до банківської системи країни. Проведений в межах наукового дослідження аналіз ефективності функціонування електронного бізнесу, дозволив дійти висновку, що зовсім не безпідставно більшість аналітиків

вважають основним гальмівним чинником електронного банкінгу негативне ставлення користувачів до нього [1].

Суттєву допомогу у вирішенні цих проблем, як свідчить світовий досвід, може надати створення та впровадження в практику банків послуг системи управління ризикованістю електронних фінансових послуг. Це забезпечить зростання обсягів електронних послуг, і, відповідно, позитивно вплине на розвиток економіки. А, відтак, виявлення та усунення гальмівних чинників ризиків розвитку та запровадження в практику українських банків систематичних та ефективних електронних послуг є нагальною проблемою.

Аналіз останніх досліджень. При написанні роботи було здійснено огляд літературних та інших інформаційних джерел, періодичних видань вітчизняних та закордонних авторів, що досягли суттєвих результатів у теорії та удосконаленні практики електронного бізнесу: П. Лисаковський [6], А. Газда [7], Я. Гжехнік [2], М.С. Деменков [3], О. Зайцев [4], А. Краевая [5], Г. Юрчук [8] тощо. Здійснено аналіз основних законодавчих та нормативних актів, що регламентують функціонування електронного бізнесу в Україні.

Метою наукової роботи є окреслення основних концептуальних засад забезпечення безпеки електронного бізнесу банку, аналіз гальмівних чинників розвитку е-бізнесу і на цій основі виявлення можливих шляхів підвищення ефективності функціонування е-банкінгу в Україні.

Виклад основного матеріалу. Електронний бізнес нині суттєво впливає на економіку і права громадян, а відтак, розбудова та входження України до світового інформаційного простору набуває надзвичайної гостроти та актуальності, рівно як і питання інформаційної безпеки в інформаційно-телекомунікаційних системах країни.

Нині стан захисту національних інформаційних ресурсів та систем викликає занепокоєння у всьому світі. Зважаючи на невпинне розширення мережі користувачів та спрощення процедури доступу до Internet збільшується кількість загроз як для комп'ютерних систем, так і для фінансової організації у цілому. Особливе занепокоєння сьогодні викликає практично стихійний розвиток та використання мережі Internet, що створює сприятливі передумови для використання її можливостей злочинними угрупованнями. Західні фахівці та експерти констатують вкрай важкий стан інформаційної безпеки у фінансових структурах, їх неспроможність протистояти можливим кібер-атакам на інформаційні системи. За оцінкою Комітету ООН з попередження злочинності і боротьби з нею, комп'ютерна злочинність вийшла на рівень однієї з головних міжнародних проблем [9]. Кібер-атаки сьогодні відбуваються як на приватні та державні компанії так і на рахунки приватних осіб. У США цей вид злочинної діяльності за прибутковістю займає третє місце після торгівлі зброєю і наркотиками, а втрати від кібер-атак сьогодні досягли 1 трлн доларів США. І дедалі крадіжки в Інтернет поширюються і набувають загрозливих масштабів. Тому питання кібер-безпеки щодо захисту банківських електронних он-лайн систем сьогодні є найважливішим при їх організації. Спеціалісти США в сфері безпеки констатують, що в зниженні ризикованності вирішальну роль сьогодні відіграє спроможність виявлення технічного засобу – джерела кібер-зламу.

Сьогодні фінансовим організаціям слід ретельно аналізувати кібер-загрози та фінансові збитки від впливу цих негативних факторів на різні автоматизовані технології сучасних інформаційних систем. Як свідчать дослідження, ймовірності реалізації випадкових загроз превалюють над навмисними (комп'ютерними злочинами, що здійснюються людиною), котрі реалізуються внаслідок несанкціонованого доступу. При цьому фінансові збитки реалізації навмисних загроз значно перевищує втрати від випадкових, ненавмисних загроз. Переважно, у більшості випадків (до 90%) зловмисником або злочинцем є співробітник брокерської контори чи банку.

Поширення комп'ютерної злочинності у фінансовій сфері пояснюється тим, що саме цій сфері належать величезні фінансові кошти, які у першу чергу цікавлять злочинців. Слід зазначити, що правоохоронним органам стають відомі далеко не всі випадки викрадення грошей шляхом використання комп'ютерних систем. До суду доходять менше, ніж 1% порушень. Це пояснюється по-перше, небажанням керівництва банків та інших організацій надавати відповідну інформацію через побоювання "компрометації" фінансових установ, а відтак оприлюднювати ризикованість своїх операцій, по-друге, можливістю виявлення додаткових правопорушень при проведенні слідчих дій, по-третє, технічною складністю розкриття комп'ютерних злочинів.

Дослідження свідчать – фінансові втрати, що пов'язані з порушенням безпеки інформаційних ресурсів, мають пряме відношення до інформаційних чи комп'ютерних ризиків. А відтак комп'ютерна система банку повинна бути захищена від спроб проникнення у неї ззовні. Якість та надійність такого захисту для Інтернет-

банкінгу є важливим фактором його існування та розвитку. Дані та процес передачі інформації між клієнтом та банком повинні бути ефективно захищені від фальсифікацій, від ситуацій, коли сторона, яка передає інформацію, могла б заперечити факт їх передачі. Крім цього, внутрішні системи користувачів повинні бути захищені від доступу до них з боку уповноважених осіб. Світове співтовариство вирішує завдання щодо забезпечення інформаційної безпеки, обираючи її раціональний рівень виходячи з економічної доцільності. 1990 року Міжнародна організація зі стандартизації (ІСО) почала створювати міжнародні стандарти критеріїв оцінки безпеки інформаційних технологій для загального використання, що мають назву "Common Criteria" чи "Загальні Критерії Оцінки Безпеки ІТ". Загальні Критерії (ЗК) є основою для незалежної оцінки інформаційної безпеки ІТ, внаслідок чого дозволяють провести порівняння результатів у світовому масштабі. Здійснюється це шляхом висування і забезпечення загальних вимог до засобів безпеки систем ІТ, а також до припустимих ризиків.

Головні переваги ЗК – повнота вимог інформаційної безпеки, гнучкість у застосуванні і відкритість для наступного розвитку з урахуванням новітніх досягнень науки і техніки. Цей стандарт може бути використаний як керівництво при розробці систем безпеки ІТ, а також при придбанні комерційних продуктів з такими системами. Основні положення стандарту сконцентровано на загрозах, що виникають внаслідок дій людини, злочинних чи інших, але він може бути застосований і у разі виникнення загроз, що не викликані діями людини. Сьогодні провідні фірми-виробники обчислювальної техніки і телекомунікацій різних країн світу проводять роботу щодо створення нової архітектури безпеки інформації для комерційних автоматизованих систем з урахуванням визначених критеріїв, а також навчальних програм, що сприяють швидкому і якісному впровадженню цих документів.

Вважаємо вкрай необхідним розробку та впровадження аналогічних до ЗК вимог і для фінансової сфери, зокрема, спеціалізованих вимог для захисту операцій електронного банківського бізнесу. Застосування загальних критеріїв оцінки безпеки інформаційних фінансових, і зокрема, банківських технологій, що відображають новітні світові досягнення оцінки інформаційної безпеки, дозволить:

- залучити вітчизняні ІТ до сучасних міжнародних вимог з інформаційної безпеки, що, зокрема, спростить застосування закордонної продукції;

- полегшити створення відповідних вітчизняних спеціалізованих нормативно-методичних матеріалів для іспитів, оцінювання (контролю) і сертифікації засобів та систем з погляду безпеки банківських й інших ІТ;

- створити основу для якісної і кількісної оцінки інформаційних ризиків, необхідну при страхуванні автоматизованих систем і, зокрема, банківських;

- знизити загальні витрати на підтримку режиму інформаційної безпеки в банках за рахунок типізації й уніфікації методів і засобів захисту інформації.

Аналіз стану захисту інформації в банківських інформаційних системах України свідчить, що появі загроз для інформації під час її обробки сприяють такі фактори:

- намагання комерційних та окремих державних структур безконтрольно, не скоординовано, створювати виділені або корпоративні телекомунікаційні системи;

- здійснення інвестиційної політики в галузі інформатизації та телекомунікацій, здебільшого без ретельного аналізу її наслідків, а також без урахування інтересів державної безпеки та оборони;

- використання в інформаційних системах несертифікованого обладнання та програмного забезпечення;

- недооцінка значущості захисту інформації та недостатньо розвинута система підготовки і перепідготовки кадрів у сфері інформаційної безпеки;

- брак чітко сформульованого і систематизованого законодавства з питань захисту і безпеки.

Слід констатувати та прийняти до уваги, що за відсутності сьогодні світових стандартів в сфері електронних фінансових послуг банкам та іншим фінансовим організаціям слід будувати власну політику безпеки електронного банківського бізнесу та власні системи управління ризиками, ретельно дотримуючись основних вимог щодо забезпечення максимального зниження рівня ризиків електронних банківських послуг. У самих банках проблеми захисту повинні зважуватися постійно, повинні існувати спеціальні відділи або окремі співробітники, що займаються безпекою Інтернет-банкінгу.

Аналіз світового досвіду дозволяє дійти висновку, що сьогодні переважна більшість банків, які пропонують свої послуги в Інтернеті, будують інформаційний захист на технології мікропроцесорних карток, а також цифрового підпису із застосуванням алгоритмів RSA, DES, 3DES [1] у

всій системі [6]. Для шифрування передачі даних, системи використовують протоколи рівня передачі даних, що забезпечує захищені з'єднання між web-сервером і броузером клієнта, зокрема, SSL протокол (Secure Sockets Layer), який забезпечує надійний Інтернет-зв'язок. Протокол SSL визнано загальним стандартом кодування веб-сторінок. Основні можливості цього протоколу: шифрування переданих даних, аутентифікация клієнтом сервера і сервером клієнта. У системах Інтернет-банкінгу використовується, як правило, вбудована в браузер клієнта реалізація SSL. Протокол HTTPS (захищений протокол передачі даних), як правило, використовується для важливих фінансових транзакций.

Під час передачі даних за допомогою протоколу SSL банки широко використовують симетричний алгоритм RC4 з довжиною ключа 128 бітів, і одночасно – асиметричний алгоритм RSA з довжиною 1024 біти [9]. Ці методи вимагають використання цифрових ключів, які служать для генерування підписів в електронних документах. Комбінація приватного та публічного ключів виключає можливість заперечення факту відправлення документа. Управління ключами повинна здійснювати інституція громадської довіри [6].

Сьогодні банки повинні забезпечити такі види безпеки системи електронного банкінгу, як показано на рис. 1.

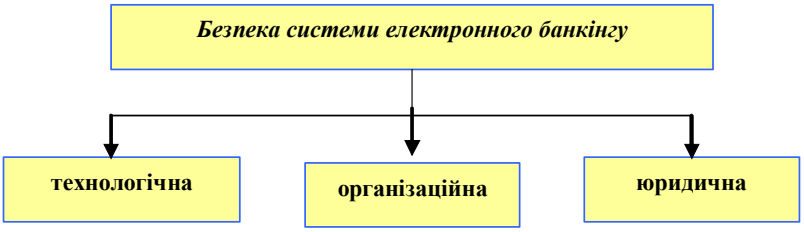

Рис. 1. Поділ безпеки системи електронного банкінгу
Джерело: www.ebanki.info

Технологічну безпеку забезпечують системи електронного банкінгу, вбудовані в телекомунікаційну інфраструктуру банку. Серед найбільш популярних систем цієї інфраструктури можна назвати інформаційні інструменти, призначені для виявлення несанкціонованих процесів у мережі, маршрутизації та постійного контролю за комунікаційними пакетами. Зростаючу небезпеку підслуховування адрес серверів і мережевих пристроїв можна усунути шляхом кодування IP-номерів у комунікаційних пакетах.

Організаційна безпека полягає у використанні приміщень з відповідним оснащенням та необхідними процедурами доступу. Спеціальну процедуру повинна пройти організація експлуатації та розвитку програмного забезпечення, котра базується на розподілі праці стосовно експлуатації та розвитку. Додатково кожне запровадження нової системи або зміна попередньої – це період детальних тестувань, подальша експлуатація яких залежить від їх результату. За дотриманням встановлених процедур повинна стежити незалежна від інформаційних груп аудиторська перевірка. Також важливим технічним рішенням є організаційна політика банку у галузі безпеки. Вона обмежується максимально звуженим колом осіб, котрі мають безпосередній доступ до "серця системи" (при цьому застосовується принцип "мінімально необхідних повноважень" – кожна особа мусить мати лише такі права доступу, які їй необхідні для роботи); підготовка аварійних процедур, а також регулярні тестування і модернізація систем паралельно з розвитком техніки. Саме у цьому напрямку повинні працювати банки, які надають послуги у мережі [7].

Юридична безпека, у свою чергу, полягає у відповідності функціонування систем електронного банкінгу чинному законодавству. У будь-яких договорах, підписаних між банком і фірмами, що займаються запровадженням та наданням послуг, повинні міститись записи про штрафи та відшкодування за недотримання умов договорів. У договорах з клієнтами останні зобов'язані ретельно ставитися до свого майна, у тому числі до криптографічних ключів, а також повинні правильно заповнити і надіслати у банк бланк електронного доручення (рис. 2) [1].

Сьогодні існують різні методи захисту інформації систем електронного банкінгу. Кожна операція може підтверджуватись введенням низки цифр, що генеруються на сервері банку, періодично змінюються (напр. кожних 60 секунд) і виводяться на екран жетона – спеціального електронного пристрою. Деякі жетони додатково можуть бути захищені паролем і у разі кількаразового неправильного введення пароля вони блокуються.

Для захисту даних під час їх передачі через Інтернет, а також правильної ідентифікації використовується весь *спектр криптографічних процедур*. Для забезпечення безпеки банки використовують кілька способів кодування. Перший з них – це криптографія, що базується на симетричних

Рис. 2. Методи захисту інформації
Джерело: www.ebanki.info

ключах. Цей спосіб передбачає застосування таємного коду, призначеного для кодування та розкодування інформації. Основною перевагою цього способу є його швидкість, продуктивність та стійкість до "зламу". Однак, як свідчить практичний досвід, цей спосіб має і певні недоліки:

- по-перше, повинен існувати спосіб безпечної передачі ключа, оскільки у разі його розкриття, вся кореспонденція стає незахищеною;

- по-друге, обидві сторони повинні довіряти одна одній і бути впевненими, що жодна з них не надасть ключа у сторонні руки;

- по третє, відсутня можливість перевірки – чи закодована інформація насправді надходить від певної особи.

Оскільки, як уже зазначалося, супроводження банківських Internet-послуг ризиками перетворює словосполучення "Інтернет" і "платежі" для багатьох компаній у синонім слова "небезпека", слід констатувати, що основним методом захисту залишається захист трансакції, який полягає у поєднанні кількох криптографічних методів, що застосовуються під час передачі, ідентифікації клієнта та його електронного підпису [7].

За відсутності безпосереднього контакту з учасниками Інтернет-зв'язку, необхідно використовувати техніку, яка би давала змогу правильно ідентифікувати відправника, встановлювати можливі спроби зміни змісту інформації під час передачі, заперечувати твердження відправника, що він не отримав інформації, або що вона мала інший зміст. Ідея електронного підпису тісно пов'язана з асиметричним алгоритмом кодування [2]. Якщо інформація буде закодована за допомогою приватного ключа, тобто посвідчена електронним підписом, тоді адресат, володіючи публічним ключем відправника, може її розкодувати і бути впевненим, що інформація походить саме від цієї особи, оскільки єдиною особою, котра володіє приватним ключем, є його власник. Такий ключ може бути записаний на криптографічній картці [9]. При функціонуванні процедури електронних підписів одержувач повинен знати публічний ключ відправника. При цьому одержувач повинен бути впевнений у тому, що цей ключ насправді належить цьому власнику. Для цього призначені електронні сертифікати [2].

Сьогодні ефективним є застосування у банках 128-бітних ключів, які використовуються один раз для кожної сесії. Дослідження підтверджують, що злам 128-бітного ключа, за умови використання способу, який був використаний для злам 40-бітного коду за всім годин, необхідно витратити мільйони років. На даний момент усі версії популярних проекторів оснащені технологією SGC (Server Gated Cryptography), завдяки якій існує можливість застосування 128-бітного кодування.

Як свідчить практика, за умов застосування банками всіх зазначених вище заходів безпеки найслабшою ланкою системи безпеки залишається комп'ютер клієнта. А, відтак, перевірка всіх процесів, ініційованих клієнтом, повинна вестися на всіх рівнях повноважень, які мають клієнт та адміністратор. З метою безпеки у системі може бути передбачено кілька паролів: для входу в систему і перегляду виписок по рахунках, для санкціонування здійснення платежів. В системі встановлюють обмеження на суму однієї операції, операцій протягом дня і протягом місяця. В операційних системах захист стосується каталогів і файлів щодо можливості їх зміни та знищення. Під час з'єднання з мережею виникає велика небезпека з боку програм, які можуть спробувати перейняти контроль над аплікацією Інтернет-банкінгу або витягнути з неї конфіденційну інформацію. Найбільшою загрозою тут є так звані "троянські коні" – програми, які передаються мережею, і які користувач запускає, не знаючи про їх скриті функції. Однією з таких функцій може бути контроль передачі мережею даних, введених за допомогою клавіатури.

Однією з ролей банку є навчання клієнтів основам безпеки, якнайбезпечнішому використанню свого рахунку в Інтернет і необхідності пам'ятати про необхідні заходи захисту:

- після роботи з фінансовим сервером не

рекомендується відразу ж переходити на інші. Необхідно закрити програму або взагалі відключити комп'ютер. Оптимальним було би використання спеціального комп'ютера, призначеного лише для фінансових операцій;

- для входження у програму зловмиснику необхідно довідатися ключ. Тому зберігати ключ у пам'яті комп'ютера не рекомендується. Ключ може бути записаний на відповідний носій, що вимагає до себе відповідального відношення, як до печатки організації чи секретних документів;

- для захисту від внутрішніх зловмисників у системі передбачені протоколи, що фіксують кожну спробу входу і всі дії. При підозрі клієнт може заблокувати ключ. Вручення нового ключа повинно відбуватись лише особисто – це виключає можливість блокування старих ключів від імені клієнта та одержання нових від сторонніх осіб;

- Інтернет-банкінг використовує до семи рівнів захисту. Тому, навіть якщо клієнт на якомусь з них вчинив неправильні дії з погляду безпеки, зловмиснику необхідно буде подолати решту шість;

- не рекомедується відповідати на листи від банку, що запитують клієнта пароль або особисті дані (PIN платіжних карт, паролі в систему, кредитний ліміт, останні покупки, дані паспорту). Слід зв'язатись з банком телефоном і перевірити справжність листа;

- рекомедується здійснювати он-лайн покупки аналогічно, як у звичайному магазині. Якщо сайт викликає підозру, слід покинути цей сайт, перевірити його законність у вашому банку або здіснювати покупки в іншому місці;

- слід переконатися, що є можливість зв'язатися з продавцем у спірних випадках, слід перевірити, чи дійсний його номер телефону;

- якщо клієнт користується інтернетом у громадських місцях, йому слід переконатися, що ніхто не може підглянути пароль. Комп'ютер завжди слід залишати у безпечному режимі, перш ніж відлучитися на певний час;

- не слід змінювати секретну інформацію (наприклад, паролі) у громадських місцях;

- не рекомедується обирати паролі, пов'язані з датою свого народження або членів родини. Буквенно-цифрові паролі вважаються безпечнішими. Паролі не слід записувати;

- обов'язковим є використання антивірусного програмного забезпечення або файєрвола;

- якщо є підозра, що пароль розкритий, слід змінiти його негайно;

- якщо є підозра, що особиста інформація розкрита, слід негайно зв'язатись з банком.

Банківські служби безпеки в Україні суттєву увагу сьогодні приділяють питанням фізичного захисту. Питання ж комп'ютерної безпеки залишаються в компетенції служб супроводження і впровадження програмного забезпечення. Кваліфікованих розробників програмного забезпечення і системних програмістів у таких службах досить багато, але фахівців у сфері систем комп'ютерної безпеки практично немає. Саме тому невід'ємною складовою державної політики, спрямованої на захист інформаційних ресурсів держави та захист інформації з обмеженим доступом, охорона якої передбачена законодавством, має стати підготовка фахівців у сфері захисту інформації та інформаційної безпеки, як складової інфраструктури інформатизації галузей національної економіки.

Система підготовки національних кадрів для роботи у сфері інформаційної безпеки та захисту в Україні та її правова підтримка потребують негайного вдосконалення. Підготовку і перепідготовку фахівців із питань технічного захисту інформації вищі навчальні заклади України до середини 1990-х років не проводили. За відповідним фахом у деяких ВНЗ України навчання почалося тільки після створення Державної служби з питань технічного захисту інформації. Підготовка фахівців у сфері інформаційної безпеки має ґрунтуватися на системному підході, що дозволить структурувати і порівнювати різні технічні, природничо-наукові та інші фахи і спеціалізації у сфері інформаційної безпеки залежно від того, за яким призначенням будуть у майбутньому працювати випускники. При цьому слід ураховувати дефіцит науково-педагогічних кадрів для вищих навчальних закладів і науково-дослідних установ. Завдання підготовки висококваліфікованих фахівців треба вирішувати в межах системи підготовки, перепідготовки і підвищення кваліфікації у сфері інформаційної безпеки та захисту інформації. Такий підхід сьогодні в Україні лише формується.

Міністерство освіти і науки України повинно координувати діяльність ВНЗ, що ведуть підготовку з інформаційної безпеки для створення цілісної системи освіти. Це дозволить об'єднати й активізувати діяльність ВНЗ і зацікавленних міністерств та відомств з підготовки та перепідготовки фахівців з інформаційної безпеки.

Висновки. Досягнення інформаційної безпеки електронного бізнесу – це один зі стратегічно важливих напрямів національної безпеки держави. Розробка національної нормативної бази, її гармонізація з міжнародними інституціями – приведення відносин у сфері інформаційної безпеки у відповідність до світових стандартів і

норм, сприятимуть зміцненню національної безпеки України та підвищенню її міжнародного авторитету як демократичної і правової держави.

Для успішного розвитку систем Internet-banking в Україні, окрім упровадження їх у банках, необхідне адекватне тлумачення таких операцій відповідними контрольними і наглядовими відомствами – НБУ, ПФ, ДПА, СБУ та іншими учасниками регулювання безготівкових розрахунків в Україні. Інакше через правовий вакуум у сфері Internet в українському законодавстві банки не подолають ризику ведення свого бізнесу через глобальну мережу.

При виборі засобів безпеки та інформаційного захисту важливо і необхідно застосовувати наукові методи, що дозволяють вибрати таку сукупність засобів захисту, яка забезпечить максимізацію рівня безпеки інформації при певних витратах або мінімізацію витрат при заданому рівні безпеки інформації.

З метою протидії фінансовим кібер-злочинам у сфері глобальних інформаційних систем та комп'ютерної інформації, а відтак, зменшення збитків від них потрібно:

- грамотно вибирати заходи і засоби забезпечення захисту інформації від просочування та несанкціонованого доступу до неї;

- знати та керуватись в роботі основними законодавчими положеннями в цій галузі, застосовувати організаційні, програмно-технічні та інші заходи забезпечення безпеки інформації;

- кваліфіковано підходити до побудови системи захисту інформації в банківських інформаційних системах, передбачаючи конкретну оцінку ймовірності виявлення кожної кібер-загрози в конкретній банківській системі;

- кожному банку, залежно від конкретних умов його роботи, потрібна персональна система захисту інформації. Побудова такої системи можлива лише на аудиторських та аутсорсингових умовах спеціально залученими фахівцями і фірмами, які мають ліцензію на цей вид діяльності.

Реалізація запропонованих заходів дасть змогу прискорити та ефективно розв'язати проблему підвищення рівня інформаційної безпеки, а відтак і ефективності електронного бізнесу в інтересах особи, суспільства, держави.

1. А. Газда: Умови безпеки сучасного електронного банкінгу, "Банк", № 9/1999. – С. 38.

2. Я. Гжехнік: Банкінг, "Банк", № 11/2001. – С. 111.

3. Деменков М.С. Інтернет-технології в обслуговуванні клієнтів банку [Текст] / М.С. Деменков // Банківська справа. – 2009. – № 1. – С. 58

4. Зайцев О. Уязвимая информация // Банковская практика за рубежом. – 2008. – №5. – С. 78 – 86

5. Краевая А. Интернет-банкинг по-украински // Банковская практика за рубежом. – 2008. – № 5. – С. 44 – 49.

6. П. Лисаковський: Кібернетична економіка по-польськи, "Банк", №10/1997. – С. 65.

7. Страхарчук А.Я., Страхарчук В. П. Інформаційні системи і технології в банках: Навч. посібник. – К.: УБС НБУ, 2010. – 515 с

8. Юрчук Г. Мережа Інтернет – сучасний канал і середовище надання фінансових послуг // Вісник Національного банку України. – 2002. – № 7. – С. 52 – 58.

9. Інтернет-джерело: Сервіс електронних банків. 05.12.2004. [http://www.ebanki.pl/banki/kanal_www.htm].

Стаття надійшла до редакції 08.09.2011

Джерела мудрості

"До вивчення наук веде подвійний шлях – авторитет та розум. У відношенні до часу (тобто в історичній традиції) панує авторитет, а у відношенні до суті справи – розум. Авторитет буває частково божественний, частково людський, але істинний, міцний та найвищий авторитет є той, який зветься божественним".

Августин Аврелій,
богослов раннього християнства, церковний письменник