УДК 004.056:336.7(477)

Матковський А.П., канд. техн. наук

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ФІНАНСОВІЙ СФЕРІ ЯК ЕЛЕМЕНТ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Львівський державний інститут новітніх технологій та управління ім. В. Чорновола

Проведено дослідження аспектів функціонування фінансової сфери та проблем забезпечення інформаційної безпеки. Виявлено основні рівні ухвалення рішень в системі забезпечення фінансової безпеки, та механізми забезпечення фінансової безпеки країни. Дослідження полягає в вивченні теоретичних положень, методологічних принципів та розробці практичних рекомендацій з інформаційної безпеки у фінансовій сфері

Об'єктом дослідження – система забезпечення інформаційної безпеки в фінансовій сфері. Предмет дослідження складають технологічні системи та організаційні, управлінські механізми захисту інформації та забезпечення інформаційної безпеки:

– для досягнення мети необхідно виконати наступні завдання;

– дослідити та проаналізувати теоретичні та методологічні основи організації захисту інформації в фінансовій сфері;

– виявити фактори інформаційної безпеки як елементів економічної безпеки держави;

– провести аналіз заходів, які застосовуються в Японії;

– розробити пропозиції стосовно формування інформаційної безпеки в фінансовій сфері виходячи з обґрунтування необхідності впровадження цих заходів.

Стрімкий розвиток науки, технології, інформаційних технологій, глобалізаційних та інтеграційних процесів приводить до того, що постає питання про інформаційну безпеку. Інформаційні технології мають великий вплив на світове суспільство та економіку. Зазначимо, що інформаційні технології включають повний діапазон інформації та технологій зв'язку, пов'язаних з інфраструктурою мереж та комп'ютерними технологіями. Інформаційні технології та глобальна мережа Інтернет з урахуванням переваг відкритості та доступністю здійснюють певний вплив на сучасні методи зв'язку та бізнесу. Цілком очевидно, що стрімкий розвиток інформаційних технологій є результатом зростання швидкості світових процесів у всіх сферах життєдіяльності суспільства (як на мікро, так й на міжнародному рівні). Інформаційні технології присутні в кожному аспекті життєвих сфер. Головні проблеми безпеки пов'язані з інформацією та технологіями її отримання, обробки, накопичення, збереження, аналізу та використання.

Це питання набуває особливої актуальності у світлі перманентних реформ, які відбуваються постійно. Інформаційно-технологічна революція суттєво змінює характер економіки в світі, що підтверджується появою нових послуг та нових інструментів бізнесу: електронна комерція, електронні платежі, нові форми банківських та фінансових послуг.

У фінансових установах існує два підходи до захисту інформації:

Автономний – направлений на захист конкретної дільниці або частини інформаційної системи, яка як правило є найбільш вразливою або може бути джерелом зловживань.

Комплексний – захищає інформаційну систему в цілому, всі її складові частини, приміщення, персонал тощо.

Важливим елементом попередження комп'ютерних злочинів у фінансовій діяльності стає застосування сучасних технічних засобів захисту інформації (під захистом розуміється обмеження доступу чи використання всієї або частини комп'ютерної системи). У Положенні про технічний захист інформації в Україні за-

значено: технічний захист інформації з обмеженим доступом в автоматизованих системах і засобах обчислювальної техніки спрямовано на запобігання порушенню цілісності інформації з обмеженим доступом та її просочення шляхом:

– несанкціонованого доступу;

– приймання й аналізу побічних електромагнітних випромінювань і наводок;

– використання закладних пристроїв;

– впровадження комп'ютерних вірусів та іншого впливу.

Технічний захист інформації з обмеженим доступом в автоматизованих системах і засобах обчислювальної техніки, призначених для формування, пересилання, приймання, перетворення, відображення та зберігання інформації, забезпечується комплексом конструкторських, організаційних, програмних і технічних заходів на всіх етапах їх створення й експлуатації.

Перш за все, ІТ прискорюють розповсюдження інформації і зменшують витрати. Це спричиняє істотні зміни методів і способів ведення бізнесу між корпораціями і стосунків між корпораціями і споживачами. Більш того, ІТ принесли більше розділення інформації в межах корпорацій, скоротили витрати на обслуговування її ієрархічної структури і істотно збільшили ефективність ділових дій. При використанні глобального мережевого ринку «бізнес-бізнесу» (B2B) компанії можуть купити сировину або комплектуючі у постачальника, який запропонує найнижчу ціну, або організувати виробництво на новому місці – в будь-яких зручних регіонах і містах, що підвищить продуктивність і знизить витрати. Наприклад, малі і середні підприємства Японії, які беруть участь на B2B ринку в Інтернеті, тепер находять партнерів безпосередньо в Азії.

Крім позитивних моментів (скорочення потреб в робочій силі, мінімізація витрат часу та коштів на здійснення всіх операцій, пов’язаних з комерційною діяльністю від пошуку інформації, партнерів, продукції до здійснення операцій навіть на світовому рівні) широке застосування інформаційних технологій призводить до появи багатьох негативних аспектів: розширення сектору тіньової економіки, шахрайство, неконтрольовані та нефіксовані дії суб’єктів, небезпека приватної інформації. Тому питання про безпеку інформації в фінансовій сфері актуальне.

Українська економіка має ярко виражені боргові риси. Україна постійно відчуває дефіцит фінансових ресурсів. Фінансова система й фінансові відношення в Україні слабо захищенні від впливу різного роду загроз й ця нестабільність набуває системного характеру. Фінанси є каналом проникнення, котрий дозволяє контролювати країну зовні. Зовнішній контроль починає розповсюджуватися не тільки на економічну, але й на соціальну сферу держави.

Таким чином, можуть з'являтися нові форми васалітету і колоніалізму [1]. Фінансова система стає саме тією часткою економіки країни, відчутно може підривати державний суверенітет. Саме тому актуальним стає питання про створення системи фінансової безпеки держави в цілях забезпечення стійкого розвитку економічної системи за допомогою визначення і моніторингу погроз фінансовій безпеці, розподілу фінансових ресурсів для підтримки необхідного рівня відтворення, незалежності і конкурентоспроможності в системі міжнародних фінансів.

Наступний елемент задає цілі, організаційні, функціональні і нормативно-правові умови, забезпечує розміщення і переміщення компонентів системи, у тому числі фінансових ресурсів за допомогою нормативно-правового регулювання. Елементи дії проходять через елементи забезпечення фінансової безпеки. До елементів забезпечення безпеки ми відносимо моніторинг слабкості (конкурентних недоліків) і погроз фінансовій системі і фінансовим стосункам; фінансово безпечне управління грошовими потоками; державний фінансовий контроль з боку

законодавчих і виконавчих органів влади, а також нормативно-правове регулювання, аналіз і контроль.

І в той самий час система, знаходиться перебуває під впливом вищезгаданих компонентів, динаміки економічного зростання, фінансового стану держави і його інститутів. Проте, ця система характеризується наявністю певних суб'єктів забезпечення фінансової безпеки: власної інфраструктури і органів державних, законодавчих і виконавчих влад, інструментів і методів забезпечення фінансової безпеки. Таким чином, позначена система здатна забезпечувати фінансову безпеку в тому випадку, якщо здатна рішати наступні проблеми:

1. Виявлення можливих загроз фінансовій безпеці.

2. Вироблення заходів по їх запобіганню.

Мета управління у сфері забезпечення фінансової безпеки – запобігання і зниження до допустимого рівня ризик виникнення загроз у фінансовій сфері.

Відповідно до вищесказаного, виділяємо наступні завдання системи забезпечення фінансової безпеки:

1. Захист державних інтересів.

2. Збір, обробка і аналіз інформації, необхідної для визначення різних проявів негативного впливу фінансових і економічних стосунків на фінансово-економічну систему.

3. Ухвалення рішень і здійснення заходів для нейтралізації і запобігання погрозам фінансовій безпеці.

У загальному вигляді управління системою забезпечення фінансової безпеки повинно включати два рівні ухвалення рішень: державний і регіональний, а також відповідні механізми забезпечення фінансової безпеки: політичні, правові, адміністративні і економічні. Для кожного з рівнів мають бути визначені відповідні повноваження по ухваленню рішень: на державному рівні, наприклад, управління зовнішніми і внутрішніми факторами, що несуть загрозу, а на регіональному – в основному внутрішніми факторами.

Фінансовий бізнес передбачає, що швидка відповідь на запити клієнта – основа обслуговування, тому все більше фінансових установ використовують Інтернет. Але розширення використання відкритих систем у фінансовому секторі послуг збільшує ризики безпеки інформації (БІ). Це вимагає нових заходів для управління ризиками фінансових установ. Зараз всі фінансові установи Японії і їх філії входять в єдину міжбанківську комп'ютеризовану мережу, що дозволяє оперативно проводити кредитно-грошові операції практично в будь-якій точці країни. Японські фінансові установи освоїли заходи безпеки, які базуються на використанні закритих систем із звичайними універсальними комп'ютерами наступного типу:

– фізичне розділення через управління входом і виходом в обчислювальний центр при будівництві мереж з виділеними лініями;

– використання спеціального програмного забезпечення і протоколів зв'язку;

– використання контролюючих камер безпеки і людського спостереження в галузі.

При вживанні таких заходів порушення безпеки із зовнішнього боку були відносно рідкі в закритих системах. Проте, при просуванні до відкритих систем почастішали випадки несанкціонованого доступу ззовні і видобування даних. Внутрішні системи обробки документів фінансових установ з'єднуються з іншими зовнішніми мережами і використовуються спільні протоколи зв'язку. Крім того, є багато пристроїв, обслуговуючих операції клієнтів, які можуть управлятися фінансовими установами менш ефективно, чим банкомати або автоматичні касові апарати. В результаті виникли ризики несанкціонованого доступу до внутрішніх систем (вторгнення хакерів) і переривання обслуговування. Більш того, істотно виросли ризики типу:

– незаконного придбання персональних кодів ідентифікації (*PIN* код);

– крадіжки даних в мережі;

– несанкціонованих грошових переказів шляхом зміни даних;

– придбання фондів при знеособлених операціях.

У Японії збільшується число фінансових установ, які постраждали від порушення БІ. Крім того, зростає число випадків переривання обслуговування, що виникає при перевантаженнях мережі постачальника мережевих послуг, що може викликати катастрофічні наслідки при операцій або передачі фондів і відбивається на діяльності не лише окремої фінансової установи, але і всієї галузі.

Останнім часом фінансові установи використовували різноманітні засоби для передачі інформації своїм філіям або спеціалізованим фірмам в інших місцях. В результаті з'являється ризик інформаційних витоків. Виникає необхідність розробки запобіжних засобів, що гарантують, що установи приймуть власні заходи безпеки, включаючи роз'яснення суворих умов в контрактах про передачу інформації і прав ревізії системи і інші гарантії.

Результати, які можна отримати внаслідок вироблення політики БІ:

1. Усвідомлення важливості БІ співробітниками організації, особливо її провідною ланкою і залучення необхідних ресурсів для реалізації заходів БІ.

2. При формулюванні заходів безпеки відповідно до послідовних стандартів забезпечення єдиного рівня БІ в межах всієї організації.

3. Виявлення слабких місць в заздалегідь здійснених заходах БІ стане простіше, а розуміння ризик буде полегшено. Наприклад, форелектронні розрахункові мережі (*ATMS*) – інший важливий електронний механізм платежів в Японії. Банки і інші депозитні установи будують свої власні мережі *CD/ATM*, а кожна мережа пов'язана з іншими через центральну систему *MICS*. Депоненти всіх приватних фінансових установ можуть отримати свої внески в будь-якому пункті *CDS/ATMS* Японії [4].

Сумісність з міжнародними стандартами.

У зв'язку з глобалізацією економіки фінансові установи Японії зіткнулися з необхідністю гарантувати, що їх політика в області БІ сумісна з міжнародними стандартами. Для досягнення цієї мети в країні використовують міжнародні стандарти і провідні принципи, прийняті міжнародними організаціями по стандартизації. Вкажемо найбільш значимі [2]:

1. *BS* 7799. Британські Стандарти. Зведене правило для управління БІ.

2. *ISO/TR*13569. Банківська справа і зв'язані фінансові послуги. Провідні принципи БІ.

3. *ISO*15408. Інформаційна технологія – методи безпеки – критерії оцінки IT безпеки

Висновки

Сьогодні в епоху стрімкого науково-технологічного розвитку набуває значної актуальності інформаційна безпека, особливо в фінансовій сфері. Адже саме фінансові ресурси є кровоносною системою держави й забезпечують не тільки її внутрішнє функціонування, але й відповідне місце на міжнародній арені.

Фінансові установи, що використовують IT для розвитку бізнесу, повинні усвідомити важливість безпеки інформації. Враховуючи бурхливий прогрес технічних нововведень, не можна дати однозначних рекомендацій по інформаційній безпеці для кожної фінансової установи. Виходячи з результатів нашого дослідження, Банк Японії підтримує дії фінансових установ по забезпеченню інформаційної безпеки і стежить за рівнем технічного прогресу в цій сфері, вимагаючи того ж від керівників кожної організації. Банк має намір безперервно тримати під контролем стан інформаційної безпеки у фінансових установах і сприяти її вдосконаленню, включаючи проведення експертиз із акцентом на безпеку інформації.

Таким чином, можна зробити висновок, що питання про інформаційну безпеку дуже гостро стоїть для України. Система інформаційної безпеки виступає

як система, що здійснює безпосередній вплив на фінансовий стан і фінансову безпеку держави, динаміку економічного зростання, фінансові пропорції і фінансову рівновагу.

У загальному вигляді управління системою забезпечення фінансової безпеки повинне включати два рівні ухвалення рішень: державний і регіональний, а також відповідні механізми забезпечення фінансової безпеки: політичні, правові, адміністративні і економічні. Для кожного з рівнів мають бути визначені відповідні повноваження по ухваленню рішень: на державному рівні, наприклад, управління зовнішніми і внутрішніми чинниками, що несуть загрозу, а на регіональному – в основному внутрішніми чинниками.

Список літератури

1. Public key identification and electronic authentication in the financial industry // IMES, Bank of Japan, 1999, Paper Series 99-J-30 (Japanese).

2. Status and issues of digital time-stamping technology // IMES, Bank of Japan, 1999, Paper Series 99-J-36 (Japanese).

3. Status and issues of personal authentication technologies through biometrics // IMES, Bank of Japan, 1999, Paper Series 99-J-43 (Japanese).

4. The importance of information security for financial institutions and proposed countermeasures // Bank of Japan, Apr. 2000.

5. *Козицын А.А.* Экономическая безопасность территории с градообразующим предприятием [Текст]: автореферат диссертации на соискание ученой степени канд. экон. наук :08.00.04,08.00.05 / А.А. Козицын. – Екатеринбург, 2000. – 28 с.

6. *Овчинский С.С.* Оперативно-розыскная информация / Овчинский С.С. – М.: Инфра-м, 2000. – 367 с.

7. *Оокоси Т.* Оптоэлектроника и оптическая связь. / пер. с япон. А.А. Генина, под ред. и с пред. М. И. Беловолова. – М.: Мир, 1988. – 96 с.

8. Проблемы защиты информации, предаваемой по волоконно-оптическим линиям связи, от несанкционированного доступа / [*Корольков А. В., Кращенко И. А., Матюхин В. Г., Синев С.* Г.] – Информационное общество. 1997. – № 1. – С. 74–77.

9. *Раздина, Е. В.* Экономическая безопасность: сущность и тенденции развития [Текст]: автореферат диссертации на соискание ученой степени канд.экон.наук: 08.00.01 / *Е. В. Раздина*. – М., 1998. – 22 с.

10. *Усманов Р.А*. Информационные основы предварительного расследования / Усманов Р.А. – М.: Юрлитинформ, 2006. – 204 с.

Подано до редакції 22.04.10