Економічні науки

УДК 336.71:65.012.8.004

Асташов Віталій Вікторович

студент

Київського національного університету технологій та дизайну

Асташов Виталий Викторович

студент

Киевского национального университета технологий и дизайна

Astashov Vitalii

Student of the

Kyiv National University of Technology and Design

ФОРМУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ
ФОРМИРОВАНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА
FORMING A SYSTEM OF INFORMATION SECURITY BANK

Анотація. *У статті розглянуто сучасні тенденції розвитку інформаційної безпеки, досліджено проблеми захисту інформації, визначено ключові фактори становлення та розвитку інформаційної безпеки банківської установи.*

Ключові слова: *інформаційна безпека, банк, захист інформації, управління, ризик, інформаційно-комунікаційні технології.*

Аннотация. *В статье рассмотрены современные тенденции развития информационной безопасности, исследованы проблемы защиты информации, определены ключевые факторы становления и развития информационной безопасности в учреждении банка.*

Ключевые слова: *информационная безопасность, банк, защита информации, управление, риск, информационно-комуникационные технологии.*

Summary. *The current trends of information security are described, the problems of information protection are investigated, the key factors of formation and development of the information security in banking system are identified.*

Key words: *information security, bank, information protection, controlling, risk, information and communication technology.*

У сучасному світі питання інформаційної безпеки вимагають підвищеної уваги, оскільки, за результатами дослідження PWC, середній збиток великих організацій від кібератак становить близько 5 млн. дол. У зв'язку з цим забезпечення захисту інформації стає особливо пріоритетним завданням, в яке бізнес інвестує дедалі більше ресурсів [1].

Згідно з прогнозами компанії Gartner, у 2015 році витрати корпорацій на IT-безпеку збільшаться на 8,2 % і сягнуть 76,9 млрд. дол. [2].

Питання захисту власної інформації є надзвичайно актуальним на сьогодні. Це зумовлено великою кількістю різноманітних кібернетичних атак та спроб зловмисників викрасти цінну інформацію з банку з метою отримання конкурентних переваг. Вже давно всім відомо, що той хто володіє інформацією та вміє правильно її використовувати здатен вивести власний бізнес на абсолютно новий рівень розвитку. Сюди можна віднести абсолютно різну інформацію, наприклад: інформацію про стан ринку фінансових послуг, інформацію про конкурентів, їх партнерів та клієнтів. Володіння такою інформацією дає змогу виключи конкурентів з боротьби за ринкову нішу зіпсувавши їхню репутацію через викрадення конфіденційної інформації.

Сьогодні дуже багато банківських установ втрачають своє конкурентне положення на ринку саме тому, що вони втрачають власну цінну інформацію, не віддаючи належного значення створенню ефективної системи

інформаційної безпеки. Дуже багато керівників не бачать потреби витрачати додаткові кошти на забезпечення захисту власних цінних даних, вважаючи, що загроза витоку даних – це явище зовсім далеке від сфери їхньої діяльності.

За останні роки дуже багато банків стали жертвами зловмисників, втратили власну конфіденційну інформацію та понесли через це значні фінансові збитки. Це зумовлено такими основними проблемами, що сьогодні наявні в сфері інформаційної безпеки:

- Відсутність єдиної державної стратегії розвитку у сфері інформаційної безпеки та єдиного державного органу, який би в масштабах країни координував пов'язані з інформаційною безпекою та IT питання в цілому, що не дозволяє створити ефективну систему захисту інформації та стримує розвиток системи управління IT та електронного уряду.
- Застаріла система національних стандартів захисту інформації. Так, для
- технічного захисту інформації застосовується так звана Комплексна система захисту інформації [3, 4], згідно з якою систему потрібно один раз побудувати, потім спеціальні організації перевіряють її і видають сертифікат про безпеку. Іншими словами з плином часу система залишається незмінною, що не гарантує фінансово обґрунтованих і надійних заходів захисту.
- Відсутність обміну інформації про кібератаки на державні організації, приватні підприємства тощо, що унеможливлює їх детальне дослідження і розроблення відповідних заходів протидії таким нападам.

Питання формування ефективної системи захисту інформації є дуже актуальним для будь-якого підприємства чи компанії, для банку воно є просто життєво необхідним. Сформувати таку систему можливо двома способами: скориставшись послугами фахівців у сфері захисту інформації або створити таку систему власними силами, перший спосіб дорожчий, але

при цьому процес формування проходить набагато швидше, другий спосіб є відносно дешевшим, але і процес створення такої системи буде відбуватися довше.

При створенні системи інформаційної безпеки в банківській установі варто визначити пріоритети захисту цінної інформації та керуватися ними в процесі. До таких пріоритетів можна віднести:

- створення служби безпеки банку;
- програмно-технічну захищеність інформації;
- інформаційну надійність персоналу;
- якість інформації, що надається для прийняття управлінських рішень[5].

Службу безпеки банку потрібно формувати не лише з точки зору фізичного захисту банку та його працівників. Потрібно враховувати, що службу безпеки не рекомендовано формувати лише з силовиків, звісно вона буде добре захищати банк від різноманітних фізичних загроз, проте економічні загрози інформаційній безпеці можуть залишитися не поміченими. Варто це враховувати та запросити на роботу висококваліфікованого економіста, який вміє добре аналізувати всі процеси, які відбуваються в економічному полі та вчасно ідентифікувати різноманітні загрози, що дозволить вчасно попередити таку загрозу або мінімізувати збитки від неї [6].

Програмно-технічна захищеність інформації є надзвичайно важливими аспектом успішної роботи банку. Проте варто зазначити, що потрібно постійно контролювати те, які захисні програми встановлюються, вчасно їх оновлювати і при можливості не користуватися послугами компаній супроводу, а взяти на роботу спеціаліста з організації роботи комп'ютерних систем, що дозволить вчасно ідентифікувати загрози програмному середовищу де знаходиться цінна інформація та закрити можливі канали її витоку.

Ще одним показником, який є дуже важливим для ефективної роботи системи захисту інформації є інформаційна надійність персоналу банку. В наш час конкуренти часто користуються різноманітними важелями впливу на співробітників, які потенційно можуть володіти цінною інформацією: підкуповувати їх, погрожувати та шантажувати. З метою запобігання втрати інформації таким способом потрібно, створити таку інформаційну систему де працівники банку не будуть володіти необмеженим доступом до цінної інформації, що в свою чергу дозволить мінімізувати ризик втрати інформації та захистити співробітників від різноманітних нападів з боку конкурентів чи шахраїв. Також потрібно лояльно відноситися до персоналу, добре оцінювати їх індивідуальні та колективні досягнення, та надавати їм можливість розвиватися і просуватися по кар'єрним сходам, адже варто пам'ятати, що не завжди потрібно залякувати чи шантажувати людину для того, щоб вона розкрила цінну інформацію [7].

Висновки. Формування системи управління інформаційної безпекою та її ІТ-підтримка в банківській сфері є важливою складовою забезпечення ефективності процесів функціонування як окремих банків, так і банківської системи в цілому. При цьому стратегія управління інформаційною безпекою повинна органічно входити не лише до складу системи управління банком, а й задовольняти загальну стратегію розвитку банківської системи відповідно до критеріїв системності та комплексності.

Варто завжди пам'ятати, що для успішного розвитку необхідно вживати заходів, яких потребує та чи інша ситуація. Створити ефективну систему захисту інформації це лише половина справи, її необхідно постійно підтримувати на високому рівні, адже ризик втрати життєво важливої для ведення бізнесу інформації існує завжди.

Література

1. Янковский А. 5 Ключових проблем в сфері інформаційної безпеки [Електронний ресурс] / А. Янковский. — Режим доступу : http://cripo.com.ua.
2. Don't Be the Next Target — IT Security Spending Priorities 2014 [Електронний ресурс]. — Режим доступу : https://www.gartner.com
3. Кіслов Д. В. Інформаційні війни.
4. Бєгун А.В. Щодо питань про сучасні методи регулювання безпеки.
5. Шакіна Д.Н. Інформаційна безпека. Зброя і технології.
6. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України : лист НБУ від 03.03.2011 № 24-112/365 [Електронний ресурс] / НБУ — Режим доступу : http://zakon4.rada.gov.ua
7. Прокопенко Н.С. Складові безпеки банківської діяльності.