

Устенко С.В.
*д.е.н., професор ДВНЗ “Київський національний
економічний університет ім. В. Гетьмана”*
kafise@ukr.net
Гіваргізов Інвія
*ДВНЗ “Київський національний економічний
університет ім. В. Гетьмана”*
hevarhizov.inviya@gmail.com

КРИТЕРІЙ ТА АНАЛІЗ ЗАСОБІВ ЕКОНОМІКО-МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ АДАПТИВНОГО РОЗВИТКУ БАНКІВ

Основні фінансові, інвестиційні та кредитні інститути України займають банки, які безпосередньо явно і неявно кредитують всіх учасників ринку. Умови стійкого розвитку банків обтяжуються незавершеністю процесу трансформації банківського сектора та недостатнім досвідом діяльності українських банків в умовах трансформації банківського сектору.

Стійкість банків серед зовнішніх та внутрішніх економічно-фінансових та операційних ризиків в першу чергу повинна забезпечуватись завдяки безпеці інформаційних ресурсів банку. Основний інформаційний інструмент банку, це його автоматизована банківська система.

Для організації системи захисту інформаційних ресурсів банку, використовують комплексну систему захисту інформації (КСЗІ) - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Мета КСЗІ є забезпечення захисту інформації, що оброблюється в автоматизованій банківській системі.

Функції КСЗІ насамперед це:

Реалізація політики безпеки інформації заданої в банківських установах;

Ідентифікація та автентифікація користувачів і надання їм доступів до інформаційних ресурсів;

Ефективне попередження та своєчасне виявлення загроз та знешкодження їх.

Відповідно до принципу абстракції при проектуванні АБС розробники можуть йти щонайменше двома шляхами: від апаратури «вгору» - до віртуальної машини, що представляє АБС, або від віртуальної машини «вниз» - до реального обладнання. Це і є два основні методи проектування - метод «знизу-вгору» і метод «зверху-вниз». Решта методів за своєю суттю зводяться до цих двох або є їх поєднанням. [1]

Перший метод досить простий, вимагає набагато менших капітальних вкладень, але і володіє меншими можливостями. Він заснований на відомій схемі: «Ви - зловмисник. Ваші дії?». Тобто служба інформаційної безпеки, ґрунтуючись на даних про всі відомі види атак, намагається застосувати їх на практиці з метою перевірки, а можливо така атака з боку реального зловмисника.

Метод «зверху-вниз» є, навпаки, детальний аналіз всієї існуючої схеми зберігання і обробки інформації. Першим етапом цього методу є, як і завжди, визначення, які інформаційні об'єкти і потоки необхідно захищати. Далі слід вивчення поточного стану системи інформаційної безпеки з метою визначення, що з класичних методик захисту інформації вже реалізовано, в якому обсязі і на якому рівні. На третьому етапі проводиться класифікація

всіх інформаційних об'єктів на класи відповідно до її конфіденційності, вимогами до доступності та цілісності. Далі слід з'ясування наскільки серйозної шкоди може принести банку розкриття або інша атака на кожен конкретний інформаційний об'єкт. Цей етап носить назву «обчислення ризиків». [1, 2]

Окрему увагу слід приділити стрес-тестуванню банків, як для передчасного пошуку та усунення проблем фінансового стану банку для стійкого розвитку в майбутньому, тому очевидна доцільність комплексного підходу до стрес-тестів повинна сприяти формуванню єдиного підходу до управління різними ризиками, адже в кризовій ситуації одночасно реалізуються й взаємно підсилюються різнорідні ризики: Коливання валютних курсів, затримками платежів по корпоративних кредитах, вилучення клієнтських ресурсів, що створює екстремальне навантаження на банківську систему.

Стрес-тестування – це загальний термін, що поєднує групу методів оцінки впливу на фінансове становище організації несприятливих подій, обумовлених як “виняткові, але можливі” [3].

Стрес-тестування широко використовується для оцінки ризику ліквідності, валютного ризику та ризику зміни процентної ставки.

Стрес-тестування – тестування чутливості або сценарне тестування з метою оцінки готовності страховика до можливих кризових ситуацій [3].

Специфіка методики “стрес-тестування” від МФВ і Світового банку реконструкції та розвитку відбита в назві її основного об’єкта аналізу – подій з низькою ймовірністю й значним впливом [4]. Такі події складно піддаються статистичній оцінці й прогнозуванню, однак їх наслідки під час управління ризиками неможливо ігнорувати. Так, виходячи зі ступеня ймовірності аналізованих подій, методи оцінки ризиків можуть розроблятися у відповідності з ієрархією нижченаведених ймовірностей:

- Аналіз ймовірно-невизначених подій;
- Аналіз найбільш імовірних подій;
- Аналіз помірно-несприятливих подій;
- Аналіз надзвичайних подій (“виняткових, але можливих”).

Очевидно, що вищенаведені методи стрес-тестування віддзеркалюють тенденцію зменшення, тобто попередній метод “поглинає” наступний за принципом зменшення невизначеності.

Враховуючи світовий досвід щодо здійснення стрес-тестування та рекомендації, які викладені в основних принципах ефективного банківського нагляду, розроблених Базельським комітетом з банківського нагляду, банкам доцільно здійснювати стрес-тестування за такими ризиками:

- Кредитний ризик;
- Ризик ліквідності;
- Ринковий ризик;
- Операційний ризик.

Для стійкого розвитку банків в першу чергу потрібно проводити аналіз існуючих фінансових, інформаційних, та економічних показників банку, і опираючись на ці показники створювати стратегію для подолання стагнації, проблем та недоліків існуючої системи розвитку банку.

Список використаних джерел

1. Grizkevich M. S. Modeling methods of capital adequacy: stress-testing / M. S. Grizkevich, I. I. Gromova., 2013. – 71 с.
2. Safety of banking activity [Electronic resource] // lutsk national technical university - Mode of access to the resource: <http://elib.lutsk-ntu.com.ua/book/fof/bs/2011/11-15/>.
3. Berlach A.I. Business Security: Teaching. - К.: University "Ukraine", 2007. - 280 p.
4. Results of stress tests of European banks [Electronic resource]. - Mode of access: www.prostobankir.com.ua