ГЛАВА 4
РИЗИКИ У БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

Керування ризиками розглядається нами на адміністративному рівні ІБ, оскільки лише керівництво банку здатне виділити необхідні ресурси, ініціювати й контролювати виконання відповідних програм.

Загалом кажучи, керування ризиками, так само як і вироблення власної політики безпеки, актуально тільки для тих організацій, інформаційні системи яких й/або оброблювані дані можна вважати нестандартними. Звичайний банк цілком улаштує типовий набір захисних заходів обраних на основі подання про типові ризики або взагалі без усякого аналізу ризиків.

Використання інформаційних систем пов'язане з певною сукупністю ризиків. Коли можливий збиток неприйнятно великий, необхідно прийняти економічно виправдані заходи захисту. Періодична (пере)оцінка ризиків необхідна для контролю ефективності діяльності в області безпеки й для обліку змін обстановки. З кількісної точки зору рівень ризику є функцією ймовірності реалізації певної загрози (використовуючи деякі уразливі місця), а також величини можливого збитку.

Таким чином, суть заходів щодо керування ризиками полягає в тому, щоб оцінити їхній розмір, виробити ефективні й економічні заходи зниження ризиків, а потім переконатися, що ризики укладені в прийнятні рамки (і залишаються такими).

Отже, керування ризиками містить у собі два види діяльності, які чергуються циклічно:

– (пере)оцінка (вимір/ризиків);

– вибір ефективних та економічних захисних засобів (нейтралізація ризиків).

Стосовно виявлених ризиків можливі наступні дії:

– ліквідація ризику (наприклад, за рахунок усунення причини);

зменшення ризику (наприклад, за рахунок використання додаткових захисних засобів);

– прийняття ризику (і вироблення плану дії у відповідних умовах);

– переадресація ризику (наприклад, шляхом висновку страхової угоди).

Процес керування ризиками можна розділити на наступні етапи:

1. Вибір аналізованих об'єктів і рівня деталізації їхнього розгляду.
2. Вибір методології оцінки ризиків.

3. Ідентифікація активів.

4. Аналіз загроз та їхніх наслідків, виявлення уразливих місць у захисті.

5. Оцінка ризиків.

6. Вибір захисних заходів.

7. Реалізація й перевірка обраних заходів.

8. Оцінка залишкового ризику.

Етапи 6 та 7 відносяться до вибору захисних засобів (нейтралізації ризиків), інші – до оцінки ризиків.

Уже перелік етапів показує, що керування ризиками – процес циклічний.

Власне кажучи, останній етап – це оператор кінця циклу, що пропонує повернутися до початку.

Ризики потрібно контролювати постійно, періодично проводячи їхню переоцінку.

Відзначимо, що сумлінно виконана й ретельно документована перша оцінка може істотно спростити наступну діяльність.

Керування ризиками, як і будь-яку іншу діяльність в області інформаційної безпеки, необхідно інтегрувати в життєвий цикл інформаційної системи (ІС). Тоді ефект виявляється, найбільшим, а витрати - мінімальними.

Раніше ми визначили п'ять етапів життєвого циклу.

Коротко опишемо, що може дати керування ризиками на кожному з них.

На етапі ініціації відомі ризики варто врахувати при виробленні вимог до системи взагалі й засобів безпеки зокрема.

На етапі розробки знання ризиків допоможе вибрати відповідні архітектурні рішення, які відіграють ключову роль у забезпеченні безпеки.

На етапі установки виявлені ризики варто враховувати при конфігуруванні, тестуванні й перевірці раніше сформульованих вимог, а повний цикл керування ризиками повинен передувати впровадженню системи в експлуатацію.

На етапі експлуатації керування ризиками повинно супроводжувати всі істотні зміни в системі.

При виведенні системи з експлуатації керування ризиками допомагає переконатися в тім, що міграція даних відбувається безпечним чином.

Класифікація ризиків

Ризики, з якими зіштовхуються українські банки у своїй діяльності дуже різноманітні. Найбільш частими ризиками, що відзначають закордонні і вітчизняні фахівці, є:

– *ризики кредитні,* які полягають у непогашенні клієнтами отриманих кредитів;

– *ризики неліквідності*, тобто ризики нестачі в банку ліквідних засобів для погашення кредиту. Такий ризик, звичайно, виникає із самої діяльності банку і може виникнути в результаті зміни процентних ставок;

– *валютні ризики*, зв'язані зі зміною курсу валюти, у якій виданий чи отриманий кредит;

– *майновий ризик*. У банках зберігаються не тільки готівка, але і цінності паперової форми, платіжні картки і т.д. Існує ризик утрати цих засобів не тільки в результаті пограбування, але і зловживання з боку службовців банку;

– *адміністративний і бухгалтерський ризики*. Вони виникають у силу розмаїтості операцій, щодня здійснюваних банком. Помилка, чи перегляд можуть не тільки нанести банку великий збиток, але і погіршити його репутацію, дискредитувати його імідж;

– *інформаційний ризик.* Ефективність інформації є вирішальним чинником у боротьбі за підвищення рентабельності й адаптації банку до більш складного конкурентного оточення. Тому помилки в розробці концепції і її реалізації, запізнювання впровадження новітньої технології й освоєння усе більш складних інформаційних систем є важливим джерелом ризику, що знижує якість і ефективність банківських послуг;

– *страховий ризик.* Має місце при міжнародному кредитуванні, тобто ризик можливої зміни економічної і політичної ситуації в країні, з підприємством якої банк має справи.

Крім цих існують ще кілька груп ризиків.

Перша група - ризики, зв'язані з загальним економічним становищем у країні. Сюди відносяться:

– кон'юнктурні ризики, тобто зміна загальної економічної ситуації н країні;

– ризики поширення банкрутств, обумовлені взаємною заборгованістю підприємств, коли банкрутство боржника може викликати труднощі і навіть банкрутство кредитора;

– ризики структурних змін у галузі, коли технологічні зміни викликають потрясіння на ринках і жадають від підприємств швидкого реагування і перебудови.

Друга група – це ризики, зв'язані з фінансуванням міжнародних операцій по нерухомості. Фахівці виділяють тут кілька груп ризиків цієї категорії:

– ризики, зв'язані з якістю самого проекту. Погано розроблений проект чи проект із перемінною геометрією, коли інвестор змінює зміст первісного проекту, не завжди правильно оцінюючи свої можливості. Проекти, реалізація яких пов'язана з переломом економічної кон'юнктури чи погіршенням положення на ринку нерухомості;

– адміністративні ризики, що виникають коли втрачає силу адміністративний дозвіл на будівництво, у зв'язку зі значною затримкою реалізації проекту і початку робіт. Фінансуючи проект банки повинні уважно відноситися до цього ризику, оскільки дозвіл на будівництво може і не бути відновлено. Адміністративні ризики можуть виникати також через те, що ті чи інші проекти зв'язані з національним культурним надбанням, тому фахівці рекомендують банкам, що беруть участь чи збирається брати участь у фінансуванні таких проектів, зв'язаних з культурним чи національним надбанням країни, утримуватися від фінансування таких проектів;

– ризики, зв'язані зі співробітництвом з іноземними банками. Банки, що беруть участь у фінансуванні закордонних проектів, вважають, що вони значно зменшать свої ризики, якщо стануть членами банківського пула, що включає ведучі банки країни, у якій реалізується проект. Тут існує небезпека того, що саме на іноземний банк будуть покладені усі витрати, зв'язані з фінансуванням проекту. Тому в даному випадку варто дуже обережно йти на співробітництво з іноземними банками при реалізації проекту в тій чи іншій «ні». Тим більше, тут існує небезпека таємних угод, пулів;

– ринкові ризики, зв'язані з характеристикою і станом ринків, на яких реалізуються проекти. Тут можуть бути наступні фактори збільшення ризику:

незначна місткість ринку, у порівнянні з масштабами проекту;

– проекти, реалізовані на модних ринках, на яких часто виникає швидко минаючий спекулятивний ажіотаж. До числа таких ринків відносяться столиці східноєвропейських країн. Мати такий проект вважається гарним тоном, хоча в більшості випадків ці проекти не приводили до бажаного результату;

– ризиками володіють також проекти в зростаючих промислових центрах.

Фахівці також вважають, що при налагодженні відносин з іноземними інвесторами, що ведуть операції з нерухомістю, варто керуватися такими уміннями, як:

– проект не стає менш ризикованим, якщо інвестор залучить до нього ще одного інвестора;

– банк-кредитор, як правило, вважає, що всі зусилля варто перекладати на плечі банкірів-акціонерів. Мова йде про створення банківських об'єднань для фінансування такого проекту. Як правило, банк, що очолює банківський пул, не захищає чи не цілком захищає інтереси учасників даного пула.

Крім названих груп ризиків існують ще ризики, пов'язані з використанням інструментів грошово-кредитного і фінансового ринків, так званих дериватів чи деривативних угод. Ці угоди самі являють собою методи рахування від ризиків.

Важливу складову частину перевірки надійності підприємства зробить дослідження його балансу. Тут потрібно враховувати, однак, що причин спроможності боржника може бути багато. Дуже часто банки роблять помилки, вважаючи, що причиною неспроможності боржника є якась одна причина, а насправді таких причин може бути кілька. На основі досліджень [3, 22, 30], можна виділити наступні причини неспроможності боржника:

1. Надмірні витрати на особисті цілі.
2. Відсутність у керівництва здатності до комерційної діяльності.
3. Помилки при веденні рахунків.
4. Занадто високий рівень запасів.
5. Зниження обсягу обороту.
6. Незадовільне фінансове планування
7. Великий обсяг помилкових інвестицій.
8. Збиток від дебіторської заборгованості.

Критеріями для оцінки надійності позичальника, за рекомендацією закордонних експертів, повинні служити:

1. Компетентність і здатність керівного персоналу підприємства.

2.Продукція і послуги підприємства.

3. Фінансове положення підприємства.

Однак слід також і враховувати надійність банку.

При оцінці функціонування банку і послуг слід враховувати його конкурентоспроможність, позицію на ринку, перспективу розвитку і послуг, структуру споживачів банка підприємства і т.д.

Для оцінки фінансового положення банка слід керуватися такими критеріями, як його ліквідність, тобто здатність оплатити свої зобов'язання в термін, можливості самофінансування, доходи, фінансова сила.

Найважливішим джерелом для оцінки фінансового положення банка є його річний баланс. Однак треба пам'ятати, що за допомогою балансу можна сховати фінансове положення банка, особливо положення з доходами. На основі балансу важко установити співвідношення між термінами надходжень коштів до банку і її платежів, тим часом це співвідношення має важливе значення для оцінки ліквідності компанії. Тому ліквідність банку варто оцінювати на основі досліджень її фінансового плану.

Для розрахунку фінансової сили банку, що характеризує здатність банка здійснювати інвестиції чи погашати отримані для цієї мети кредити, необхідно аналізувати рух його готівки. Оцінка фінансової сили банка виробляється шляхом обчислення готівки у відсотках, або до обороту банка, або до земельного капіталу. Результат поділення позикового капіталу на величину готівки показує, скільки років буде потрібно банку для погашення своїх зобов'язань.

Одержання інформації для оцінки надійності позичальника повинне будуватися на двох принципах: по-перше, потрібно чітко визначити обсяг необхідної інформації, а по-друге, інформацію варто одержувати по можливості з різних і незалежних друг від друга джерел.

Аналіз ризиків

В даний час технології аналізу ризиків в Україні розвинуті слабко. Основна причина такого положення полягає в тому, що в українських керівних документах недостатньо розглядається аспект ризиків, їхній припустимий рівень і відповідальність за прийняття визначеного рівня ризиків.

Питанням аналізу ризиків за кордоном приділяється серйозна увага десятиліттями. Однак і у нас в країні положення починає змінюватись. Серед вітчизняних фахівців служб безпеки зріє розуміння необхідності проведення такої роботи. У першу чергу це відноситься до банків і великих комерційних структур, тобто до тих, хто в першу чергу зобов'язаний серйозно піклуватися про безпеку своїх інформаційних ресурсів.

Мета аналізу ризиків складається у визначенні характеристик ризиків. При проведенні аналізу ризиків необхідно визначити:

– уразливі місця в даній системі;

– сутність загрози, їхній рівень;

– припустимий рівень загроз;

– комплекс засобів, що дозволяє знизити ризики до припустимого рівня. По кожному з цих пунктів потрібно проведення спеціального аналізу і досліджень.

Режим інформаційної безпеки в банківських системах забезпечується:

– на процедурному рівні – шляхом розробки і виконання розділів інструкцій для персоналу, присвячених інформаційній безпеці, а також засобами фізичного захисту;

– на програмно-технічному рівні – застосуванням апробованих і сертифікованих рішень, стандартного набору контрзаходів: резервне копіювання, антивірусний захист, парольний захист, міжмережеві екрани, шифрування даних і т.д.

При забезпеченні інформаційної безпеки важливо не пропустити яких-небудь істотних аспектів. Це буде гарантувати деякий *мінімальний (базовий)* рівень інформаційної безпеки, обов'язковий для будь-якої інформаційної технології. У випадку підвищених вимог в області інформаційної безпеки використовується *повний варіант аналізу ризиків*. На відміну від базового варіанта, виробляється оцінка цінності ресурсів, характеристик ризиків і вразливості.

Інструментарій аналітика

Застосування яких-небудь інструментальних засобів не є обов'язковим, однак їхнє використання дозволяє зменшити трудомісткість проведення аналізу ризиків і вибору контрзаходів. В даний час на ринку є біля двох десятків програмних продуктів для аналізу ризиків: від найпростіших, орієнтованих на базовий рівень безпеки, до складних і дорогих продуктів, що дозволяють провести повний аналіз ризиків і вибрати комплекс контрзаходів необхідної ефективності.

Аналіз ризиків для базового рівня

Звичайною областю використання цього рівня є типові проектні рішення. Існує ряд стандартів і специфікацій, у яких розглядається мінімальний (типовий) набір найбільш ймовірних загроз, таких як збої устаткування, віруси, несанкціонований доступ і т.д. Для нейтралізації цих

загроз обов'язково повинні бути прийняті контрзаходи незалежно від імовірності їхнього здійснення й уразливості ресурсів. У такий спосіб програмні продукти, призначені для цієї мети, дозволяють сформувати список питань, що стосується виконання цих вимог. На основі відповідей генерується звіт з рекомендаціями з усунення виявлених загроз. Програмний продукт дозволяє представити вимоги стандартів у виді тематичних питань по окремим аспектам діяльності банку. Цей продукт може використовуватися при проведенні аудита інформаційної безпеки чи роботи фахівців служб, що відповідають за забезпечення інформаційної безпеки.

Ще однією областю застосування є перевірка на відповідність вимогам базового рівня захищеності банку. Мається можливість настроювання на різні області застосування шляхом додавання чи виключення додаткових питань. Крім того, мається калькулятор очікуваних середньорічних втрат, що дозволяє оцінити очікувані втрати по різних видах інформаційних ресурсів.

Повний аналіз ризиків

Повний варіант аналізу ризиків застосовується у випадку підвищених вимог в області інформаційної безпеки. На відміну від базового варіанта в тому чи іншому виді виробляється оцінка цінності ресурсів, характеристик ризиків і уразливості ресурсів. Як правило, проводиться аналіз вартість/ефективність декількох варіантів захисту.

Програмні засоби, що дозволяють провести повний аналіз ризиків, будуються з використанням структурних методів системного аналізу і проектування і являють собою інструментарій для:

– побудови моделі інформаційної системи з погляду інформаційної безпеки;

– оцінки цінності ресурсів;

– складання списку загроз і вразливості, оцінки їхніх характеристик;

– вибору контрзаходів і аналізу їхньої ефективності;

аналізу варіантів побудови захисту;

– документування (генерація звітів).

Обов'язковим елементом цих продуктів є база даних, яка містить інформацію з інцидентів в області інформаційної безпеки, що дозволяє оцінити ризики й уразливості, ефективність різних варіантів контрзаходів у конкретних ситуаціях. Аналіз ризиків містить у собі ідентифікацію й обчислення рівнів ризиків на основі оцінок, привласнених ресурсам, загрозам і вразливості ресурсів.

Контроль ризиків складається з ідентифікації і вибору контрзаходів, що дозволяють знизити ризики до прийнятного рівня.

Це дозволяє переконатися, що захист охоплює всю систему й існує впевненість у тім, що:

– усі можливі ризики ідентифіковані;

– уразливості ресурсів ідентифіковані і їхні рівні оцінені;

– загрози ідентифіковані і їхні рівні оцінені;

– контрзаходи ефективні;

– витрати, зв'язані з інформаційною безпекою, виправдані.

Аналіз ризиків проводиться в три етапи.

Етап 1: аналізується усе, що стосується ідентифікації і визначення цінності ресурсів системи. Наприкінці цього етапу банк буде знати, чи досить йому існуючої традиційної практики, чи він має потребу в проведенні повного аналізу безпеки.

Етап 2: розглядається усе, що відноситься до ідентифікації й оцінки рівнів загроз для груп ресурсів і їх уразливості. Наприкінці другого етапу банк одержує ідентифіковані й оцінені рівні ризиків для своєї банківської системи.

Етап **3**: пошук адекватних контрзаходів. Власне кажучи, це пошук варіанта системи безпеки, що максимально відповідає вимогам банку. Наприкінці етапу замовник буде знати, як варто модифікувати систему для відхилення від ризику, а також вибору спеціальних заходів протидії, що ведуть до зниження ризиків, що залишилися, до необхідного і припустимого рівня.

Розглянемо більш детально кожний **з** етапів.

Етап 1. Ідентифікація ресурсів і побудова моделі інформаційної системи з погляду безпеки

Основні кроки:

– визначення меж дослідження (межи системи);

– ідентифікація ресурсів (устаткування, дані, програмне забезпечення);

– побудова моделі з погляду інформаційної безпеки;

– визначення цінності ресурсів;

– одержання звіту й обговорення його з керівництвом банку.

Визначення меж дослідження

Визначення меж досліджуваної системи починається зі збору наступної інформації:

– відповідальні за фізичні і програмні ресурси;

– хто є користувачем і як користувачі будуть використовувати систему;

– конфігурація системи.

Первинна інформація збирається в процесі бесід з менеджером чи іншими співробітниками.

Ідентифікація ресурсів і побудова моделі системи з погляду інформаційної безпеки

Проводиться ідентифікація ресурсів: фізичних, програмних і інформаційних, що містяться усередині меж системи. Кожен ресурс необхідно віднести до одного з визначених класів. Потім будується модель інформаційної системи з погляду інформаційної безпеки. Для кожного інформаційного процесу, що має самостійне значення з погляду користувача і названого користувальницьким сервісом (End-User-Service), будується дерево зв'язків використовуваних ресурсів. Побудована модель дозволяє виділити критичні елементи.

Оцінювання цінності ресурсів

Цінність фізичних ресурсів визначається ціною їхнього відновлення у випадку руйнування.

Цінність даних і програмного забезпечення визначається в наступних ситуаціях:

– неприступність ресурсу протягом визначеного періоду часу;

– руйнування ресурсу – втрата інформації, отриманої з часу останнього резервного копіювання, чи її повне руйнування;

– порушення конфіденційності у випадку несанкціонованого доступу штатних чи співробітників сторонніх облич;

– модифікація розглядається для випадків дрібних помилок персоналу (помилок уведення), програмних помилок, навмисних помилок;

– помилок, зв'язаних з передачею інформації: відмовлення від доставки, недоставляння інформації, доставка по невірній адресі.

Для оцінки можливого збитку рекомендується використовувати деякі **з** наступних параметрів:

– збиток репутації банку;

– порушення діючого законодавства;

– збиток для здоров'я персоналу;

– збиток, зв'язаний з розголошенням персональних даних окремих облич;

– фінансові утрати від розголошення інформації;

– фінансові втрати, зв'язані з відновленням ресурсів;

– утрати, зв'язані з неможливістю виконання зобов'язань;

– дезорганізація діяльності.

Приведена сукупність параметрів використовується в комерційному варіанті методу. В інших версіях сукупність буде іншою. Так, у версії, використовуваної в урядових закладах, додаються такі області, як національна безпека і міжнародні відносини.

Одержання звітів і їх обговорення

На першому етапі може бути підготовлено кілька типів звітів (межі системи, модель, визначення цінності ресурсів).

Якщо цінності ресурсів низькі, можна використовувати базовий варіант захисту. У такому випадку дослідник може відразу перейти від етапу 1 до етапу 3. Однак для адекватного обліку потенційного впливу якої-небудь погрози, вразливості, що мають високі рівні, варто використовувати скорочену версію етапу 2. Це дозволяє розробити більш ефективну схему захисту.

ЕТАП 2. АНАЛІЗ ЗАГРОЗ І УРАЗЛИВОСТЕЙ

На другому етапі:

– оцінюється залежність користувальницьких сервісів від визначених груп ресурсів;

– оцінюється існуючий рівень загроз і уразливостей;

– обчислюються рівні ризиків;

– аналізуються результати.

Виробляється угруповання ресурсів з погляду загроз і вразливостей. Наприклад, у випадку існування погрози пожежі чи крадіжки як групу ресурсів розумно розглянути всі ресурси, що знаходяться в одному місці.

Оцінка рівнів загроз і уразливостей виробляється на основі дослідження непрямих факторів. Програмне забезпечення для кожної групи ресурсів і кожного з типів загроз генерує список питань, що допускають однозначну відповідь.

Можливе проведення корекції результатів чи використання інших методів оцінки.

На підставі цієї інформації розраховуються рівні ризиків. Отримані рівні загроз, вразливостей і ризиків аналізуються й узгоджуються з замовником. Тільки після цього переходять до третього етапу.

ЕТАП 3. ВИБІР КОНТРЗАХОДІВ

На цьому етапі генеруються кілька варіантів заходів протидії, адекватних виявленим ризикам і їхнім рівням. Умовно їх можна об'єднати в 3 категорії:

– рекомендації загального плану;

– конкретні рекомендації;

– приклади того, як організується захист у даній ситуації.

На цій стадії можливо провести порівняльний аналіз ефективності різних варіантів захисту.

Методологія аналізів ризиків та процесів керування ними

Одним з можливих підходів до розробки методик аналізу ризиків є нагромадження статистичних даних про події, які відбулись, аналіз і класифікація причин, виявлення факторів ризику. На основі цієї інформації можна оцінити загрози й уразливості в інших інформаційних системах.

Практичні складності в реалізації цього підходу наступні: *по-перше*, повинен бути зібраний дуже великий матеріал про події в цій області; *по-друге*, застосування цього підходу виправдано далеко не скрізь. Якщо банківська система досить велика (містить багато елементів, розташована на великій території), має давню історію, то подібний підхід виправданий. Якщо порівняно невелика, використовує новітні елементи технології (для якої поки немає достовірної статистики), оцінка ризиків і уразливості може виявитися недостовірною.

Альтернативою статистичному підходу є підхід, заснований на аналізі особливостей технології. Утім, цей підхід також не універсальний: темпи технологічного прогресу в області інформаційних технологій такі, що оцінки, що мають, відносяться до застарілих чи застаріваючих технологій, для новітніх технологій таких оцінок поки не існує.

Загроза сама по собі не несе ніякого збитку для діяльності банку: вона існує об'єктивно, потенційно, поза залежністю від нашого знання про її існування. Однак у деякий момент часу кожна загроза може перейти з потенційної в реальну, тобто реалізуватися. У цей момент часу банк вже має визначений збиток, якщо реалізація даної загрози не була вчасно відвернена, і банк має справу з коефіцієнтом збитку від реалізації даної загрози.

При виконанні методики повного аналізу ризиків приходиться вирішувати ряд складних проблем: Як визначити цінність ресурсів?

Як скласти повний список загроз інформаційної безпеки й оцінити їхні параметри?

Як правильно вибрати контрзаходи й оцінити їх ефективність? Відповідно до цього методика оцінювання ризиків містить кілька етапів:

– ідентифікація ресурсу й оцінювання його кількісних показників чи визначення потенційно негативного впливу на банківську діяльність;

– оцінювання загроз;

– оцінювання вразливості;

– оцінювання існуючих і передбачуваних засобів забезпечення інформаційної безпеки;

– оцінювання ризиків.

Ризик характеризує небезпеку, якій може піддаватися банк і інформаційна система, яка використовується банком для своєї діяльності. І при оцінюванні ризиків враховуються потенційний негативний вплив від небажаних подій і показники значимості розглянутих уразливості і загроз для них.

Ступінь ризику залежить від:

– показників цінності ресурсу;

– імовірності реалізації загроз;

– простоти використання уразливості при виникненні загроз;

– існуючих чи планованих до впровадження засобів забезпечення інформаційної безпеки, скорочують імовірність виникненні загроз і негативних впливів.

Визначення цінності ресурсів

Ресурси діляться на кілька класів, наприклад: фізичні, програмні і дані. Для кожного класу повинна існувати методика оцінки цінності елементів.

Для оцінки цінності ресурсів вибирається придатна система критеріїв. Критерії повинні дозволяти описати потенційний збиток, зв'язаний з порушенням конфіденційності, цілісності, доступності.

Цінність фізичних ресурсів оцінюють з погляду вартості їхньої заміни відновлення працездатності. Ці вартісні величини перетворяться в якісну шкалу, що використовують, також, інформаційний ресурс. Програмні ресурси оцінюються тим же що і фізичні, на основі визначення витрат на їх придбання чи відновлення.

Якщо для інформаційного ресурсу існують особливі вимоги конфіденційності цілісності, то оцінка цього ресурсу виробляється по тій схемі, тобто у вартісному вираженні.

Крім критеріїв, що враховують фінансові втрати, у банках можуть бути присутніми критерії, що відбивають:

– збиток репутації банку;

– неприємності, зв'язані з порушенням діючого законодавства;

– збиток для здоров'я персоналу;

– збиток, зв'язаний з розголошенням персональних даних окремих облич;

– фінансові утрати від розголошення інформації;

– фінансові втрати, зв'язані з відновленням ресурсів;

– утрати, зв'язані з неможливістю виконання зобов'язань;

– збиток від дезорганізації діяльності банку.

Можуть використовуватися й інші критерії в залежності від профілю банку.

Оцінка характеристик факторів ризику

Ресурси повинні бути проаналізовані з погляду оцінки впливу можливих атак (спланованих дій внутрішніх чи зовнішніх зловмисників) і різних небажаних подій природного походження. Також потенційно можливі події називаються загрозами безпеки. Крім того, необхідно ідентифікувати уразливості – слабості в системі захисту, що уможливлюють реалізацію загроз.

Для того щоб конкретизувати імовірність реалізації загрози розглядається деякий відрізок часу, протягом якого передбачається захищати ресурс. Імовірність того, що загроза реалізується, визначається наступними факторами:

– привабливістю ресурсу (цей показник враховується при розгляді загрози навмисного впливу з боку людини);

– можливість використання ресурсу для одержання доходу (показник враховується при розгляді загрози навмисного впливу з боку людини);

– простотою використання уразливості при проведенні атаки.

В даний час відома безліч методів оцінювання загроз, більшість з яких побудовані на використанні таблиць. Такі методи порівняно прості у використанні і досить ефективні. Однак не слід говорити про кращий метод, тому що в різних випадках вони будуть різними. Важливо з наявного

різноманіття методів вибрати саме той, який забезпечив би відтворені результати для даного банку.

Ранжирування загроз

У матриці чи таблиці можна наочно відбити зв'язок факторів негативного впливу (показників ресурсів) і ймовірностей реалізації загрози з урахуванням показників уразливості (табл. 4.1).

На першому кроці оцінюється негативний вплив (показник ресурсу) по заздалегідь визначеній шкалі, наприклад від 1 до 5, для кожного ресурсу, якому загрожує небезпека (стовпчик *b* у табл. 4.1.)

Таблиця 4.1

Дескриптор загрози (a)	Показник негативного виливу (ресурсу) (b)	Імовірність реалізації погрози (c)	Показник ризику (d)	Ранг загрози (e)
Загроза A	5	2	10	2
Загроза B	2	4	8	3
Загроза C	3	5	15	1
Загроза D	1	3	3	5
Загроза E	4	1	4	4
Загроза F	2	4	8	3

На другому кроці – по заздалегідь заданій шкалі, наприклад від 1 до 5, оцінюється імовірність реалізації кожної загрози.

На третьому кроці обчислюється показник ризику. У найпростішому варіанті методики це робиться шляхом множення (*bxc*). Однак необхідно пам'ятати, що операція множення визначена для кількісних шкал. Для рангових (якісних) шкал виміру, якими є показник негативного впливу й імовірність реалізації загрози, приміром, зовсім необов'язково показник ризику, що відповідає ситуації b=1, x=3, буде еквівалентний b=3, x=1. Відповідно, повинна бути розроблена методика оцінювання показників ризиків стосовно до конкретного банку.

На четвертому кроці загрози ранжируються за значеннями їхнього фактора ризику.

Оцінювання рівнів ризику.

Розглянемо метод, побудований на використанні таблиць і враховуючий тільки вартісні характеристик ресурсів.

Цінність фізичних ресурсів оцінюється з погляду вартості їхньої заміни відновлення працездатності (тобто кількісних показників). Ці вартісні величини потім перетворяться в якісну шкалу, що використовується також

для інформаційних ресурсів. Програмні ресурси оцінюються тим же способом, що і фізичні, виходячи з витрат на їхнє чи придбання відновлення.

Якщо для інформаційного ресурсу існують особливі вимоги до чи конфіденційності цілісності, то оцінка цього ресурсу виробляється по тій же схемі, тобто у вартісному вираженні.

Кількісні показники інформаційних ресурсів оцінюються на підставі опитувань співробітників банку (власників інформації) - тих хто може оцінити цінність інформації, визначити її характеристики і ступінь критичності. На основі результатів опитування виробляється оцінювання показників і ступеня критичності інформаційних ресурсів для найгіршого варіанта розвитку подій. Розглядається потенційний вплив на бізнес-процес при можливому несанкціонованому ознайомленні з інформацією, зміні інформації, відмовленні від виконання обробки інформації, неприступності на різні терміни і руйнуванні.

Далі розробляється система показників у бальних шкалах. Таким чином, кількісні показники використовуються там, де це припустимо і виправдано, а якісні - там, де кількісні оцінки неможливі.

По кожній групі ресурсів, зв'язаній з даною загрозою, оцінюється рівень останньої (ймовірність реалізації) і ступінь уразливості (легкість з якою реалізована загроза здатна привести до негативного впливу). Оцінювання здійснюється в якісних шкалах.

Поділ ризиків на прийнятні і неприйнятні

Інший спосіб оцінювання ризиків складається в поділі їх тільки на прийнятні і не прийнятні. Підхід ґрунтується на тім, що кількісні показники ризиків використовуються тільки для їх упорядкування і визначення першочергових дій. Але це можна досягти і з меншими витратами.

Матриця, використовувана в даному підході, містить не числа, а тільки символи Д (ризик допустимо) і Н (ризик не допустимо).

Кожен рядок у матриці визначається показником ресурсу, а кожен стовпець – ступенем небезпеки загрози й уразливості. Розмір матриці, що враховує кількість ступенів загроз і вразливості, категорій ресурсів, може бути іншим і визначається конкретним банком.

Світовий досвід банківської діяльності, узагальнення досвіду роботи ведучих російських і українських банків показують, що системоутворюючим елементом керування ризиками в бізнесі є інформаційно-аналітична діяльність. Саме на її базі і будується система комплексної безпеки, що

покликана виявляти і прогнозувати зовнішні і внутрішні загрози життєво важливим інтересам, а також здійснювати необхідний комплекс дій по їх попередженню і нейтралізації.

При прогнозуванні і мінімізації ризиків інформаційна підтримка має визначальне, але не виняткове значення. Для рішення проблеми необхідно почати цілий комплекс заходів, спрямований на забезпечення підприємництва й особистості. Штучне вичленовування одного з елементів комплексу (навіть найважливішого) не вирішує задачу цілком.

В даний час немає стрункої системи класифікації підприємницьких ризиків. Всі існуючі нині підходи до класифікації ризиків недостатньо повно відбивають розмаїтість ризиків, тому представляється обов'язковим визначенням їхніх типів і угруповання по визначених ознаках.

Першочерговою задачею є оцінка стану керування ризиками в банку, що припускає проходження наступних етапів:

– установлення причин, факторів, джерел ризику в банку;

– ідентифікація ризиків банку;

– побудова профілю ризику;

– інтегральна оцінка ризику банку по профілю;

– аналіз використовуваних у банку заходів щодо керування ризиками;

– оцінка ефективності застосовуваних заходів.

Дослідження стану керування ризиками проводиться при дотриманні наступних принципів:

– комплексності, що дозволяє охопити організаційні, інформаційні, виробничо-технічні, соціальні, економічні, юридичні аспекти проблеми;

– науковості, що базується на визначенні оптимального варіанта дій для досягнення поставленої задачі;

– системності, що представляє об'єкт дослідження у вигляді цілісної єдиної системи;

– прогресивності, що полягає у відповідності дослідження передовим методам і методикам вітчизняного і закордонного досвіду.

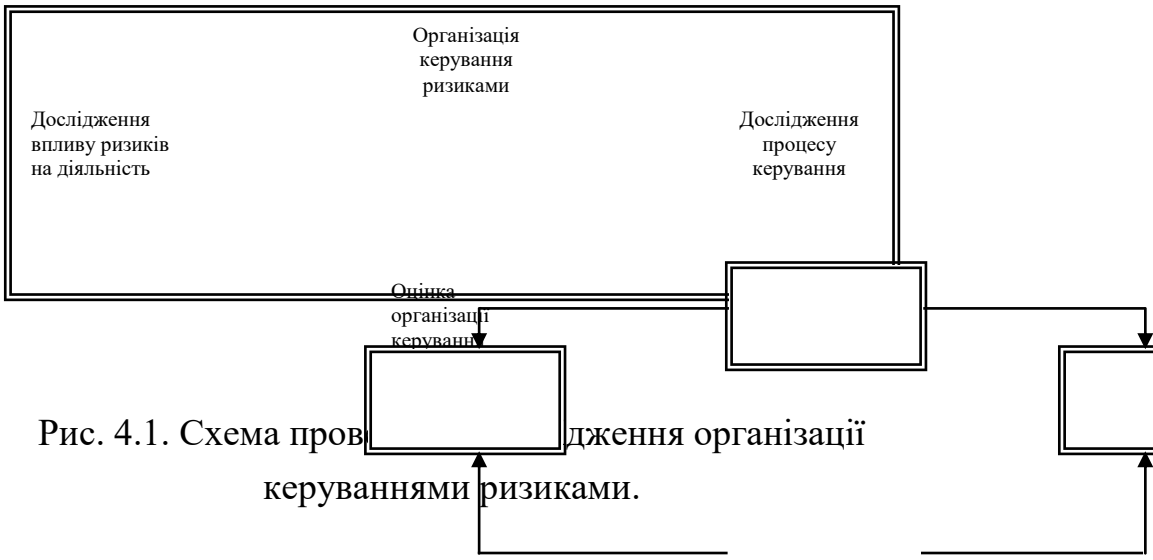

Рис. 4.1. Схема проведення дослідження організації керуваннями ризиками.

Дослідження організації керування ризиками в банку доцільно проводити в три етапи (рис. 4.1.). Розглянемо ці етапи більш детальніше.

ЕТАП І. Дослідження впливу ризиків на діяльність банків.

Проводиться послідовно з вісьмох кроків:

КРОК 1. Розпізнавання об'єкта дослідження. Метою є визначення узагальненої характеристики об'єкта, що дозволяє представити його як систему, а так само як частина системи більш високого порядку.

КРОК 2. Аналіз об'єкта. Проводиться по напрямках (рис. 4.2.):

– аналіз макросередовища;

– аналіз мікросередовища.

Проведення аналізу макросередовища здійснюється шляхом вивчення спеціалізованих СМІ про положення в галузі за попередні 3-5 років.

Для проведення аналізу мікросередовища банку, а також його безпосереднього оточення використовуються наступні документи:

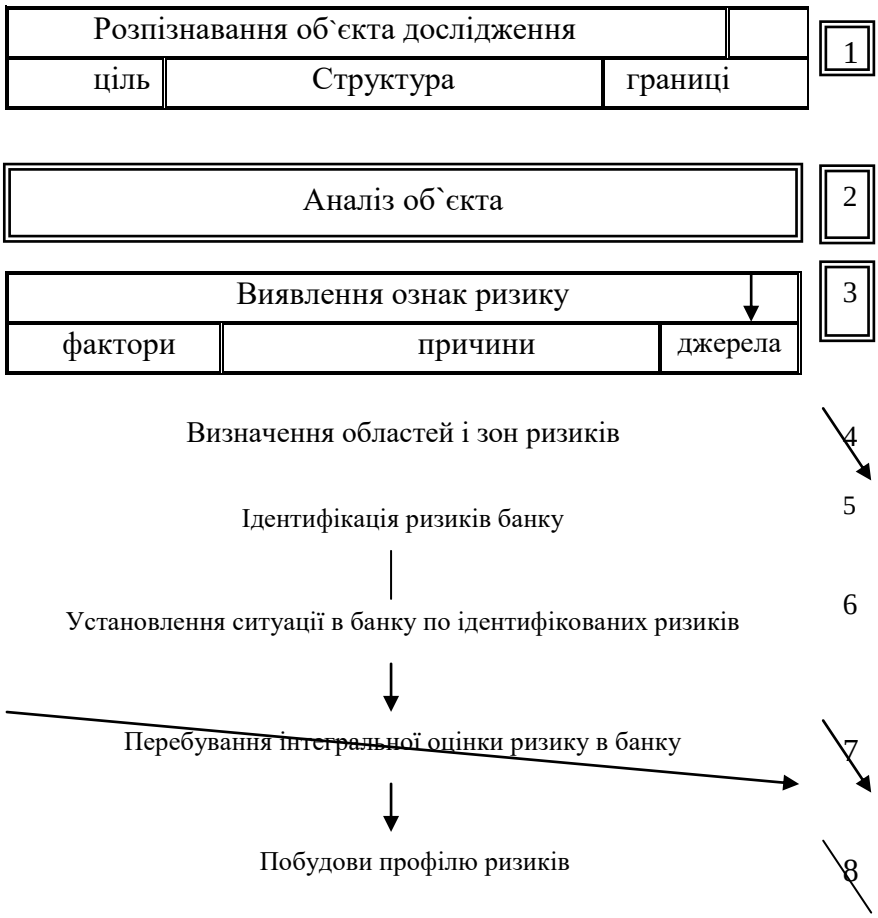

Рис.4.2. Процес дослідження впливу ризиків на діяльність банку

1) організаційно-структурна схема керування банку;

2) штатний розклад;

3) бухгалтерська звітність;

4) статут банку;

5) комплект положень про підрозділи банку;

6) комплект посадових інструкцій співробітників;

7) перелік клієнтів, договори;

8) звіти про роботу банку за попередній час, проведення аналізу за 3 роки;

9) плани роботи з удосконалювання і т.д.;

10) перелік випадків НСД (за 3 роки);

11) зведення про судові справи, арбітражах, у яких брали участь чи співробітники банку (за 3 роки);

12) список облич, що подавали заяву про звільнення;

13) список співробітників, що працюють не за основним фахом;

14) обсяг і види послуг, що робляться банком своїм співробітникам;

15) відомості про плинність кадрів;

16) відомості про штрафи;

17) дані про страхування об'єктів і т.д.

Крок 3. Виявлення ознак ризиків. За підсумками проведення аналізу (крок 2) за допомогою методу експертних оцінок виробляється визначення факторів, причин, джерел ризиків у банку. Експертам пропонується оцінити можливі джерела ризику.

За результатами опитування виробляється розрахунок середнього значення по балах, привласненими експертами наочній причині. Виходячи з цього, робиться висновок про наявність даної причині виникнення ризику в досліджуваному банку. На підставі отриманих результатів, а також представлених допусків виробляється SWOT - аналіз банку (Strength Weakness Opportunity - якісний підхід, що базується на порівнянні протилежних якостей проекту), у результаті проведення якого встановлюються сильні і слабкі сторони банку, присутні загрози і можливості по їхньому відбиттю.

Крок 4. Визначення областей і зон ризиків. Здійснюється за допомогою системно-цільового підходу.

Крок 5. Ідентифікація ризиків банку. Виробляється виявлення всіх характерних для банків ризиків відповідно до установлених факторів, причинами і джерелами ризиками, а також їхнього ранжирування. Ранжирування може бути проведено методом експертних оцінок. Кожному ризику привласнюється значимість по кількісній шкалі від 1 до 10. Максимальна оцінка відповідає найбільш значимому ризику.

Крок 6. Визначення ситуації по ідентифікованих ризиках. Визначається рівень кожного ризику (відсутність, низький, невисокий, високий) і тенденція до його зміни (зниження, збереження, збільшення).

Крок 7. Інтегральна оцінка ризику банку. Здійснюється за допомогою шкали оцінок ризиків на підставі отриманих при реалізації кроку результатів.

На основі визначеного рівня ризиків і привласнених банків визначається оцінка кожного ризику по формулі:

$$D_i = L_i \gamma_i \qquad (4.1)$$

де

D_i– оцінка *i*-го ризику;

I_i – вага *i*-го ризику;

i – бал, що привласнюється і-му ризику. Інтегральна оцінка (у) ризику дорівнює:

$$\gamma = \gamma_i \qquad (4.2)$$

де

γ – інтегральна оцінка ризику

Інтегральна оцінка ризику лежить у межах :

$$0 \leq \gamma \leq 7 \qquad (4.3)$$

КРОК 8. Побудова профілю ризиків. За отриманими оцінками необхідно провести формування груп ризиків, що відбивають специфіку банку, і установити пріоритети.

ЕТАП ІІ. Дослідження процесу керування ризиками.

Дослідження проводиться послідовно, у три кроки (рис.4.3).

КРОК 1. Виявлення ризиків у роботі банку. Визначення властивих для даного банку загроз, виявлення можливого збитку, оцінка ступеня ризиків. Ухвалення рішення про те, які ризики будуть враховуватися, а якими можна зневажити.

Рис. 4.3. Процедура дослідження процесу керування ризиками

КРОК 2. Аналіз заходів щодо керування ризиками. Аналіз здійснюється в двох напрямках:

– Аналіз можливих альтернатив (альтернативи вибираються на основі досвіду банку чи аналогічних банків);

– аналіз застосовуваних засобів (рис. 4.4.).

Рис. 4.4. Схема аналізу використовуваних засобів

Крок 3. Вибір ефективних прийомів по керуванню ризиками. Цей крок здійснюється на підставу даних табл. 4.2.

Таблиця 4.2

Засіб	Витрати	Ефективність
1	X_1	$Є_1$
2	X_2	$Є_2$
…	$X_{….}$	$Є_{….}$
N	X_N	$Є_N$

ЕТАП III. Оцінка організації керування ризиками.

Цей етап проводиться за підсумками етапів 1 і II. При оцінці організації керування ризиками необхідно розглянути структуру керування, забезпечення керування ризиками, персонал, що бере участь у процесі керування, і зв'язку, що виникають у ньому (рис. 4.5).

Рис. 4.5. Оцінка організації керування ризиками в банку

Крок 1. Аналіз структури керування ризиками. Розглядається наявність відсутності у банку організаційної і функціональної структур керування ризиками.

Крок 2. Аналіз забезпечення процесу керування ризиками. Враховується інформаційне, організаційно-правове, кадрове, фінансове, програмно-математичне, лінгвістичне і технічне забезпечення процесу керування ризиками.

Крок 3. Технологія керування ризиками. Розглядається механізм керування ризиками, що існує в банку (за підсумками етапу Н).

За результатами проведення дослідження (етапи І–Ш) робиться висновок про стан організації керування ризиками в банку.

Підготовчі етапи керування ризиками

У цьому розділі будуть описані перші три етапи процесу керування ризиками. Вибір аналізованих об'єктів і рівня деталізації їхнього розгляду – перший крок в оцінці ризиків. Для невеликої організації, припустимо, розглядати всю інформаційну інфраструктуру, однак, якщо організація велика, всеохоплююча оцінка може вимагати неприйнятних витрат часу й сил. У такому випадку варто зосередитися на найбільш важливих сервісах, заздалегідь погоджуючись із наближеністю підсумкової оцінки. Якщо важливих сервісів усе ще багато, вибираються ті з них, ризики для яких свідомо великі, або невідомі.

Ми вже вказували на доцільність створення карти інформаційної системи

організації. Для керування ризиками подібна карта особливо важлива, оскільки вона наочно показує, які сервіси обрані для аналізу, а істотно змінені сервіси мають потребу в розгляді.

Загалом кажучи, уразливим є кожен компонент інформаційної системи – від мережевого кабелю, який можуть прогризти миші, до бази даних, що може бути зруйнована через невмілі дії адміністратора. Як правило, у сферу аналізу неможливо включити кожен гвинтик і кожен байт. Доводиться зупинятися на деякому рівні деталізації, усвідомлюючи наближеність оцінки. Для нових систем кращий детальний аналіз; стара система, яка піддається незначним модифікаціям, може бути проаналізована більш поверхнево.

Дуже важливо вибрати розумну методологію оцінки ризиків. Метою оцінки є одержання відповіді на два питання: чи прийнятні існуючі ризики, і якщо ні, то які захисні засоби варто використовувати. Виходить, оцінка повинна бути кількісною, що допускає зіставлення із заздалегідь обраними межами допустимості й витратами на реалізацію нових регуляторів безпеки. Керування ризиками – типова оптимізація завдання, й існує досить багато програмних продуктів, здатних допомогти в її вирішенні (іноді подібні продукти просто додаються до книг з інформаційної безпеки). Принципові труднощі, однак, складаються в неточності вихідних даних. Можна, звичайно, спробувати одержати для всіх аналізованих величин грошовий

вираз, вирахувати все з точністю до копійки, але особливого сенсу в цьому немає. Практичніше користуватися умовними одиницями. У найпростішому й цілком припустимому випадку можна користуватися трибальною шкалою. Далі ми продемонструємо, як це робиться.

При ідентифікації активів, тобто тих ресурсів і цінностей, які організація намагається захистити, треба, звичайно, ураховувати не тільки компоненти інформаційної системи, але й підтримуючу інфраструктуру, персонал, а також нематеріальні цінності, такі як репутація організації. Відправною крапкою тут є уявлення про місію організації, у будь-якому випадку напрямки діяльності, які бажано (або необхідно) зберегти в кожному разі. Висловлюючись об'єктно-орієнтованою мовою, треба в першу чергу описати зовнішній інтерфейс організації, розглянутої як абстрактний об'єкт.

Одним з головних результатів процесу ідентифікації активів є одержання детальної інформаційної структури організації й способів її (структури) використання. Ці відомості доцільно нанести на карту ІС як межі відповідних об'єктів.

Інформаційною основою якої-небудь великої організації є мережа, тому в число апаратних активів варто включити комп'ютери (сервери, робочі станції, ПК), периферійні пристрої, зовнішні інтерфейси, кабельне господарство, активне мережеве устаткування (мости, маршрутизатори й т.п.).

До програмних активів, імовірно, будуть віднесені операційні системи (мережева, серверні й клієнтські), прикладне програмне забезпечення, інструментальні засоби, де (у яких вузлах мережі) зберігається програмне забезпечення, і з яких вузлів воно використовується. Третім видом інформаційних активів є дані, які зберігаються, обробляються й передаються по мережі. Варто класифікувати дані по типах і ступеню конфіденційності, виявити місця їхнього зберігання й обробки, способи доступу до них. Все це важливо для оцінки наслідків порушень інформаційної безпеки.

Керування ризиками – процес далеко не лінійний. Практично всі його етапи пов'язані між собою, і по завершенню майже кожного з них може виникнути необхідність повернення до попереднього.

Так, при ідентифікації активів може виявитися, що обрані межі аналізу варто розширити, а ступінь деталізації – збільшити. Особливо складний первинний аналіз, коли багаторазові повернення до початку неминучі.

Основні етапи керування ризиками

Етапи, що передують аналізу загроз, можна вважати підготовчими, оскільки прямого зв'язку з ризиками вони не мають. Ризик з'являється там, де є загрози.

Короткий перелік найпоширеніших загроз був розглянутий нами раніше. На жаль, на практиці загроз набагато більше, причому далеко не всі вони, носять комп'ютерний характер. Так, цілком реальною загрозою є наявність мишей і тарганів у займаних організацією приміщеннях. Перші можуть зашкодити кабелю, другі викликати коротке замикання. Як правило, наявність тієї або іншої загрози є наслідком недоліків у захисті інформаційної системи, які, у свою чергу, характеризуються відсутністю деяких сервісів безпеки або недоліками в реалізуючих їх захисних механізмах. Небезпека прогризання кабелів виникає не просто там, де є миші, вона пов'язана з відсутністю або недостатньою міцністю захисної оболонки.

Перший крок в аналізі загроз - їхня ідентифікація. Розглянуті види загроз варто вибирати виходячи з міркувань здорового глузду (відкинувши, наприклад, землетрус, однак не забуваючи про можливості захоплення організації терористами), але в межах обраних видів провести максимально докладний аналіз.

Доцільно виявляти не тільки самі загрози, але й джерела їхнього виникнення – це допоможе у виборі додаткових засобів захисту. Наприклад, нелегальний вхід у систему може стати наслідком відтворення початкового діалогу, підбору паролю або підключення до мережі неавторизованого устаткування. Очевидно, для протидії кожному з перерахованих способів нелегального входу потрібні свої механізми безпеки.

Після ідентифікації загрози необхідно оцінити імовірність її здійснення. Можливе використання при цьому трибальної шкали (низька (1), середня (2) і висока (3) ймовірність.

Крім імовірності здійснення, важливим є розмір потенційного збитку. Наприклад, пожежі бувають нечасто, але збиток від кожної з них, як правило, великий. Розмір збитку також можна оцінити за трибальною шкалою. Оцінюючи розмір збитку, необхідно мати на увазі не тільки безпосередні витрати на заміну устаткування або відновлення інформації, але й більш віддалені, такі як підрив репутації, ослаблення позицій на ринку й т.п. Нехай, наприклад, у результаті дефектів у керуванні доступом до бухгалтерської інформації співробітники одержали можливість корегувати дані про власну

заробітну платню. Наслідком такого стану справ може стати не тільки перевитрата бюджетних або корпоративних засобів, але й повне розкладання колективу, що може призвести до розвалу організації.

Уразливі місця мають властивість притягати до себе не тільки зловмисників, але й порівняно чесних людей. Не кожен тримається перед спокусою дещо збільшити свою зарплатню, якщо є впевненість, що це тобі минеться. Тому, оцінюючи імовірність здійснення загроз, доцільно виходити не тільки із середньостатистичних даних, але враховувати також специфіку конкретних інформаційних систем. Якщо в підвалі будинку, займаного організацією, розташовується сауна, а сам будинок має дерев'яні перекриття, то імовірність пожеж, на жаль, виявиться істотно вище середнього.

Після того, як накопичені вихідні дані й оцінений ступінь невизначеності, можна переходити до обробки інформації, тобто власне до оцінки ризиків. Цілком припустимо застосовувати такий простий метод, як множення ймовірності здійснення загрози на передбачуваний збиток. Якщо для імовірності й збитку використовувати трибальну шкалу, то можливих добутків буде шість: 1, 2, 3, 4,6 й 9. Перші два результати можна віднести до низького ризику, третій і четвертий – до середнього, два останні - до високого, після чого з'являється можливість знову привести їх до трибальної шкали. По цій шкалі й варто оцінювати прийнятність ризиків. Щоправда, граничні випадки, коли обчислювальна величина збіглася із прийнятною, доцільно розглядати більш ретельно через наближений характер результату.

Якщо які-небудь ризики виявилися неприпустимо високими, необхідно їх нейтралізувати, реалізувавши додаткові заходи захисту. Як правило, для ліквідації або нейтралізації уразливого місця, що зробило загрозу реальною, існує кілька механізмів безпеки, різних за ефективністю й вартістю. Наприклад, якщо велика імовірність нелегального входу в систему, необхідно, щоб користувачі обирали довгі паролі (скажемо, не менше восьми символів), задіяти програму генерації паролів або закупити інтегровану систему аутентифікації на основі інтелектуальних карт. Якщо є ймовірність навмисного ушкодження сервера баз даних, що може мати серйозні наслідки, можна урізати замок у двері серверної кімнати або поставити біля кожного сервера по охоронцю.

Оцінюючи вартість засобів захисту, доводиться, зрозуміло, ураховувати не тільки прямі витрати на закупівлю устаткування й/або програм, але й витрати на впровадження новинки й, зокрема, навчання й

перепідготовку персоналу. Цю вартість також можна оцінити по трибальній шкалі й потім зіставити її між обчисленим і припустимим ризиком. Якщо за цього показника новий засіб виявляється економічно вигідним, його можна взяти на замітку (підходящих засобів, імовірно, буде декілька). Однак якщо засіб виявиться дорогим, його не слід відразу відкидати, пам'ятаючи про наближення розрахунку.

Вибираючи підходящий спосіб захисту, доцільно враховувати можливість екранування одним механізмом забезпечення безпеки відразу декількох прикладних сервісів. Так зробили в Масачусетському технологічному інституті, захистивши кілька тисяч комп'ютерів сервером аутентифікації Kerberos.

Важливою обставиною є сумісність нового засобу зі сформованою організаційною й апаратно-програмною структурою, із традиціями організації. Заходи безпеки, як правило, носять недружній характер, що може негативно позначитися на ентузіазмі співробітників. Часом збереження духу відкритості важливіше мінімізації матеріальних втрат. Втім, такого роду орієнтири повинні бути розставлені в політиці безпеки верхнього рівня.

Можна уявити собі ситуацію, коли для нейтралізації ризику не існує ефективних і прийнятних за ціною заходів. Наприклад, компанія, що базується в сейсмічно небезпечній зоні, не завжди може дозволити собі будівництво захищеної штаб-квартири. У такому випадку доводиться піднімати межу прийнятного ризику й переносити центр ваги на пом'якшення наслідків і вироблення планів відновлення після аварій, стихійних лих та інших подій. Продовжуючи приклад із сейсмобезпекою, можна рекомендувати регулярне тиражування даних в інше місто й володіння засобами відновлення первинної бази даних.

Як і будь-яку іншу діяльність, реалізацію й перевірку нових регуляторів безпеки варто попередньо планувати. У плані необхідно врахувати наявність фінансових засобів і строки навчання персоналу. Якщо мова йде про програмно-технічний механізм захисту, потрібно скласти план тестування (автономного й комплексного).

Коли заплановані заходи впроваджені, необхідно перевірити пеню, дієвість, тобто переконатися, що залишкові ризики стали прийнятними. Якщо це насправді так, виходить, можна спокійно намічати дату найближчої переоцінки. У іншому випадку доведеться проаналізувати допущені помилки й провести повторний сеанс керування ризиками негайно.