

# Ризики у банківській діяльності

A close-up photograph of several credit cards, likely Visa and Mastercard, with a brass padlock resting on them. The padlock is closed and positioned centrally, symbolizing security and risk. The cards are slightly out of focus, showing embossed numbers and logos.

Лектор:

Лимаренко Вячеслав Володимирович

к.т. 066-070-8586

# Керування ризиками

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

*Керування ризиками*, так само як і вироблення власної політики безпеки, актуально тільки для тих організацій, інформаційні системи яких і 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.

# Керування ризиками

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*.

# Керування ризиками

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*).



# Керування ризиками

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).

# Етапи процесу керування ризиками

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*.

# Етапи процесу керування ризиками

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

Ризики потрібно контролювати постійно, періодично проводячи їхню переоцінку.

Сумлінно виконана й ретельно документована *перша оцінка* може істотно спростити наступну діяльність.

# Керування ризиками на п'яти етапах життєвого циклу

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

Ризики потрібно контролювати постійно, періодично проводячи їхню переоцінку.

Сумлінно виконана й ретельно документована *перша оцінка* може істотно спростити наступну діяльність.



# Керування ризиками на п'яти етапах життєвого циклу

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

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;

# Класифікація ризиків

- *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.

# Аналіз ризиків

В даний час технології *аналізу ризиків* в Україні розвинуті слабо. 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.

Серед вітчизняних фахівців служб безпеки зріє розуміння необхідності проведення аналізу ризиків. 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.

# Аналіз ризиків

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.

# Аналіз ризиків

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, виконується 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 налаштування 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).

# Повний аналіз ризиків

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.

# Три етапи аналізу ризиків

*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 вразливості. 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.

# 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.



# ЕТАП 1. ІДЕНТИФІКАЦІЯ РЕСУРСІВ І ПОБУДОВА МОДЕЛІ ІНФОРМАЦІЙНОЇ СИСТЕМИ З ПОГЛЯДУ БЕЗПЕКИ

## *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.

# ЕТАП 1. ІДЕНТИФІКАЦІЯ РЕСУРСІВ І ПОБУДОВА МОДЕЛІ ІНФОРМАЦІЙНОЇ СИСТЕМИ З ПОГЛЯДУ БЕЗПЕКИ

## *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 співробітників чи сторонніх осіб;
- модифікація розглядається для випадків дрібних помилок персоналу (помилки введення), програмних помилок, навмисних помилок;
- помилок, зв'язаних з передачею інформації: відмовлення від доставки, недоставляння інформації, доставка по невірній адресі.

# ЕТАП 1. ІДЕНТИФІКАЦІЯ РЕСУРСІВ І ПОБУДОВА МОДЕЛІ ІНФОРМАЦІЙНОЇ СИСТЕМИ З ПОГЛЯДУ БЕЗПЕКИ

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 осіб;
- фінансові утрати від розголошення інформації;
- фінансові втрати, зв'язані з відновленням ресурсів;
- утрати, зв'язані з неможливістю виконання зобов'язань;
- дезорганізація діяльності.

# ЕТАП 1. ІДЕНТИФІКАЦІЯ РЕСУРСІВ І ПОБУДОВА МОДЕЛІ ІНФОРМАЦІЙНОЇ СИСТЕМИ З ПОГЛЯДУ БЕЗПЕКИ

## *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 ВРАЗЛИВОСТЕЙ

На другому етапі:

- оцінюється залежність користувальницьких сервісів від визначених груп ресурсів;
- оцінюється існуючий рівень загроз і уразливостей;
- обчислюються рівні ризиків;
- аналізуються результати.

Виконується 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 вразливостей 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 методики 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.

# Методологія аналізів ризиків та процесів керування ними

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 наявні, 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.

## Етапи методології аналізу ризиків

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.

## Етапи методології аналізу 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, які 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 або відновлення працездатності. Ці вартісні величини перетворюються в якісну шкалу, що використовують, також, для оцінки інформаційного ресурсу. Програмні ресурси оцінюються тим же методом, 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 виконується по тій же схемі, тобто у вартісному вираженні.

## 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 вразливості – слабості в системі захисту, що уможливляють 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 прибутку (показник враховується при розгляді загрози навмисного впливу з боку людини);
- простотою використання вразливості при проведенні атаки.



## Ранжирування загроз

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

Таблиця 1

Дескриптор загрози (a)	Показник негативного впливу (b)	Імовірність реалізації загрози (c)	Показник ризику (d)	Ранг загрози (e)
Загроза А	5	2	10	2
Загроза В	2	4	8	3
Загроза С	3	5	15	1
Загроза D	1	3	3	5
Загроза Е	4	1	4	4
Загроза F	2	4	8	3

## Ранжирування загроз

**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.1).

**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 ( $b \times x$ ). 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.

**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.1).

**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 ( $b \times x$ ). 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.

## Оцінка ймовірності здійснення загроз

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

Крім ймовірності 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.

Вразливі місця мають властивість притягувати до себе не тільки зловмисників, але й порівняно чесних людей.

## Оцінка ймовірності здійснення загроз

Не кожен утримається перед спокусою дещо збільшити свою зарплатню, якщо є впевненість, що це тобі минеться. Тому, оцінюючи ймовірність здійснення загроз, доцільно виходити не тільки із середньостатистичних даних, але враховувати також специфіку конкретних інформаційних систем.

Якщо в підвалі будинку, що займається організацією, розташовується сауна, а сам будинок має дерев'яні перекриття, то ймовірність пожеж, на жаль, виявиться істотно вище середньої.

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 ймовірності 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.

## Оцінка ймовірності здійснення загроз

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, реалізуювши додаткові заходи захисту. Як правило, для ліквідації або нейтралізації вразливого місця, що зробило загрозу реальною, існує кілька механізмів безпеки, різних за ефективністю й вартістю.

Наприклад, якщо велика ймовірність 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 врізати замок у двері серверної кімнати або поставити біля кожного сервера по охоронцю.

## Оцінка вартості засобів захисту

*Оцінюючи вартість* засобів захисту доводиться враховувати не тільки прямі витрати на закупівлю устаткування 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.

## Оцінка вартості засобів захисту

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).



## Оцінка вартості засобів захисту

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.

A blue key is positioned diagonally across the frame. The background is a light blue gradient with a pattern of binary code (0s and 1s) in a darker blue, creating a digital or technological theme. The key has a circular head and a notched bit.

**Дякую за увагу**  
**Лекцію закінчено**