5.3. УПРАВЛІННЯ РИЗИКОМ ІНФОРМАЦІЙНИХ СИСТЕМ

Використання інформаційних систем пов'язане з певною сукупністю ризиків. В разі, якщо можливий збиток надто великий, необхідно вживати економічно виправдані заходи щодо захисту. Періодична оцінка ризиків необхідна для контролю ефективності діяльності в області безпеки і для обліку змін обстановки.

З кількісної точки зору рівень ризику є функцією вірогідності реалізації певної загрози (що використовує деякі вразливі місця), а також величини можливого збитку.

Таким чином, суть заходів щодо управління ризиками полягає в тому, щоб оцінити їх розмір, виробити ефективні і економічні заходи зниження ризиків, а потім переконатися, що ризики вміщені в прийнятні рамки (і залишаються такими). Отже, управління ризиками включає два види діяльності, які працюють циклічно:

- оцінка ризиків;
- вибір ефективних і економічних заходів.

По відношенню до виявлених ризиків можливі наступні дії:

- ліквідація ризику;
- зменшення ризику**;**
- ухвалення ризику**;**
- переадресація ризику**.**

Процес управління ризиками можна розділити на такі етапи:

1. Вибір аналізованих об'єктів і рівня деталізації їх розгляду.
2. Вибір методології оцінки ризиків.
3. Ідентифікація активів.
4. Аналіз погроз і їх наслідків, виявлення вразливих місць в захисті.
5. Оцінка ризиків.
6. Вибір захисних заходів.
7. Реалізація і перевірка вибраних заходів.
8. Оцінка залишкового ризику**.**

Шостий та сьомий етапи відносяться до вибору захисних засобів (нейтралізації ризиків), інші - до оцінки ризиків.

Наведений перелік етапів показує, що управління ризиками - процес циклічний. По суті, останній етап - це оператор кінця циклу, приписуючий повернутися до початку. Ризики слід постійно контролювати, періодично проводячи їх переоцінку. Відзначимо, що сумлінно виконана і ретельно задокументована перша оцінка може істотно спростити подальшу діяльність.

Для управління ризиками важливі карти інформаційної системи, оскільки вона предметно показує, які сервіси вибрані для аналізу, а якими довелося нехтувати. Якщо ІС міняється, а карта підтримується в актуальному стані, то при переоцінці ризиків відразу стане ясно, які нові або такі, що істотно змінилися сервіси, потребують розгляду.

Метою оцінки є отримання відповіді на два питання: чи прийнятні існуючі ризики, а якщо ні, то які захисні засоби слід використовувати. Оцінка повинна бути кількісною, щоб допускати зіставлення з вибраними наперед межами допустимості і витратами на реалізацію нових регуляторів безпеки. Управління ризиками - типове оптимізаційне завдання, і існує досить багато програмних продуктів, здатних допомогти в їх вирішенні (іноді подібні продукти просто додаються до книг по інформаційній безпеці). Принципова трудність, проте, полягає в неточності первісних даних. Можна, звичайно, спробувати одержати для всіх аналізованих величин грошовий вираз, вирахувати все з точністю до копійки, але великого сенсу в цьому немає. Практичніше користуватися умовними одиницями. У простому і цілком допустимому випадку можна користуватися трибальною шкалою.

При ідентифікації активів, тобто тих ресурсів і цінностей, які компанія намагається захистити, слід, враховувати не тільки компоненти інформаційної системи, але і персонал, що підтримує інфраструктуру, персонал, а також нематеріальні цінності, такі як репутація компанії. Важливо мати уявлення про місію компанії**,** тобто про основні напрями діяльності, які бажано (або необхідно) зберегти у будь-якому випадку. Виражаючись об'єктивно-орієнтованою мовою, слід, в першу чергу описати зовнішній інтерфейс компанії, що розглядається як абстрактний об'єкт.

Одним з головних результатів процесу ідентифікації активів є отримання детальної інформаційної структури компанії і способів її використання. Ці відомості доцільно нанести на карту ІС як грані відповідних об'єктів.

Інформаційною основою компаній виступає наявність мережі, тому в число апаратних активів слід включити комп'ютери, периферійні пристрої, зовнішні інтерфейси, кабельне господарство, активне мережне устаткування. До програмних активів, повинні бути віднесені операційні системи, прикладне програмне забезпечення, інструментальні засоби, засоби

управління мережею і окремими системами. Важливо зафіксувати, де зберігається програмне забезпечення, і з яких вузлів воно використовується. Третім видом інформаційних активів є дані, які зберігаються, обробляються і передаються через мережу. Слід класифікувати дані за типами і ступенем конфіденційності, виявити місця їх зберігання і обробки, способи доступу до них. Все це важливо для оцінки наслідків порушень інформаційної безпеки.

Управління ризиками - процес далеко не простий. Практично всі його етапи пов'язані між собою. Після закінчення будь-якого з них може виникнути необхідність повернення до попереднього. Так, при ідентифікації активів може виявитися, що вибрані межі аналізу слід розширити, а ступінь деталізації - збільшити. Особливо важкий початковий аналіз, в разі, якщо численні повернення до початку неминучі.

Вирішення завдань аналізу ризику можливо тільки при використанні спеціалізованих інформаційних систем, що реалізовують в собі функції зберігання й обробки масивів даних, моделювання і виконання розрахункових завдань, представлення результатів в доступній формі, вироблення порад і рекомендацій особам, котрі ухвалюють рішення щодо управління ризиками. Таким чином, для вирішення завдань управління ризиком інформаційних систем необхідна орієнтація на підтримку процесів ухвалення стратегічних рішень.

Основой інформаційного забезпечення СУР є комплекс моделей, які повинні задовольняти вимогам:

- єдність формального апарату, що використовується;
- забезпечувати побудову стратифікованого комплексу моделей, в якому кожна вершина моделі описується власною моделлю;
- забезпечувати можливість вирішення завдань аналізу і синтезу з різним числом рівнів стратифікації, яке визначається необхідною глибиною аналізу;
- забезпечувати можливість сполучення моделей по схемі вихід-вхід, в разі, якщо результат, одержаний на виході однієї моделі, є вхідним значенням для іншої;
- забезпечувати можливість виконання розрахунків від входу до виходу і від виходу до входу з обчисленням параметрів на основі комплексних критеріїв (адитивні, мультиплікативні та інші).

Як і будь-яку іншу діяльність, реалізацію і перевірку нових регуляторів безпеки слід заздалегідь планувати. У плані необхідно врахувати наявність фінансових коштів і терміни навчання персоналу. Якщо йдеться про програмно-технічний механізм захисту, потрібно скласти план тестування (автономного і комплексного).

В разі, якщо накреслені заходи прийняті, необхідно перевірити їх дієвість, тобто переконатися, що залишкові ризики стали прийнятними. Якщо це насправді так, то можна спокійно намічати дату найближчої переоцінки. Інакше доведеться проаналізувати допущені помилки і провести повторний сеанс управління ризиками негайно.