



УКРАЇНА

(19) UA (11) 35889 (13) U

(51) МПК (2006)

G06F 15/00

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ПАТЕНТУ
НА КОРИСНУ МОДЕЛЬвидається під
відповідальність
власника
патенту

(54) СПОСІБ ЗАХИСТУ ІНФОРМАЦІЙНИХ ІНФРАСТРУКТУР

1

2

(21) u200805340

(22) 24.04.2008

(24) 10.10.2008

(46) 10.10.2008, Бюл.№ 19, 2008 р.

(72) ЄРМОШИН ВАЛЕРІЙ ВІТАЛІЙОВИЧ, UA

(73) ЛЕУШ ОЛЕКСАНДР ГРИГОРОВИЧ, UA

(57) Спосіб захисту інформаційних інфраструктур, при якому системно аналізують та керують ризиками, застосовуючи центральний процесор та периферійну мережу приладів, який відрізняється тим, що додатково автоматизують аналізування та керування периферійною мережею приладів, яке

виконує центральний процесор шляхом сканування її роботи, приймання інформаційних сигналів від неї, порівняння цих сигналів із вибраним еталоном, формування та передавання на периферійну мережу керівних інформаційних сигналів для забезпечення автоматизованого захисту інформаційних інфраструктур, при цьому цю автоматизовану систему як невід'ємну частину інформаційних інфраструктур використовують протягом усього життєвого циклу діяльності цих інформаційних інфраструктур.

Корисна модель відноситься до інформаційних технологій, зокрема до способу автоматизованого захисту інформаційних інфраструктур з використанням системи аналізування ризиків та системи управління ризиками.

З розвитком інформаційних технологій зростає роль забезпечення інформаційної безпечності для ведення бізнесу тощо. Інформація із забезпечувальної функції набуває функції важливого ресурсу. Це призводить до того, що на підприємствах та в організаціях необхідно впроваджувати та підтримувати в належному стані інформаційну та інформаційно-технічну інфраструктуру, які складаються із системи організаційних структур за допомогою яких забезпечується функціонування та розвиток інформаційного простору та інформаційної взаємодії яка включає сукупність інформаційних центрів, баз даних, систем зв'язку, програмного забезпечення, локальних мереж, мереж Internet, телекомунікаційних мереж тощо. Ці структури забезпечують доступ відповідних фахівців та користувачів, в випадку коли система загальнодоступна, до інформаційних ресурсів (активів) підприємств будь якої форми власності, організації, компанії, в тому числі і транснаціональних.

Відоме застосування процесного підходу до менеджменту захисту інформації, який наведений в міжнародному стандарті ISCVIEC 27001: 2005 Information Technology - Security Techniques - Information security management systems - Requirements (www.iso.org/iso). Згідно з вимогами цього

міжнародного стандарту, ресурси (активи) повинні бути відповідним чином захищені на основі проведення оцінювання ризиків інформаційної безпеки. Основною задачею інформаційної безпеки є захист ресурсів (активів) від внутрішніх та зовнішніх навмисних чи ненавмисних загроз (підробки, вандалізму, крадіжки, системного збою тощо). Результати оцінювання ризиків необхідні керівництву для визначення пріоритетів по управлінню ризиками інформаційної безпеки і для впровадження заходів щодо захисту інформаційних інфраструктур від ризиків, які на їх думку є критичними для діяльності бізнесу. Концепції аналізування ризиків, управління цими ризиками на усіх стадіях життєвого циклу інформаційних інфраструктур були запропоновані багатьма розробниками, які займаються проблемами інформаційної безпеки.

Відомі технології оцінювання ризиків по методу CRAMM (www.cramm.com), який є універсальним інструментом для аналізування ризиків. В його основі лежить комплексний метод оцінювання ризиків, який поєднує кількісні та якісні методи аналізування. Недоліками цього методу є необхідність спеціальної підготовки та високого рівня кваліфікації фахівців які проводять аналіз, трудомісткість процесу, генерація великої кількості паперових документів що не дозволяє впровадити максимальний рівень автоматизації. Крім того, цей метод не дозволяє складати шаблони звітів які б задовольняли вимогам широкого спектру користувачів.

(13) U

(11) 35889

(19) UA

Найбільш близьким за технічною сутністю до пропонованого винаходу є відоме застосування способу захисту інформаційних інфраструктур із застосуванням комплексної системи аналізування та управління ризиками інформаційної системи ГРИФ (www.dsec.ru/products/grif). Ця система дозволяє аналізувати рівень захищеності всіх ресурсів (активів) компанії, оцінювати можливі збитки, які компанія понесе в результаті реалізації загрози інформаційній безпеці, ефективно управляти ризиками за допомогою вибору оптимальних та відповідних контрзаходів. Також, ця система дозволяє проводити аналізування ризиків інформаційних систем за допомогою моделі інформаційних потоків і моделі загроз.

Недоліком цього способу захисту інформаційних інфраструктур за допомогою аналізування ризиками є недостатній рівень автоматизації процесу аналізування та оцінки ризиків, складність процесу їх управління, необхідність високого рівня кваліфікації фахівців які проводять оцінку та управління ризиками, загальна трудомісткість процесу.

Технічна задача корисної моделі полягає в розроблянні способу захисту інформаційних інфраструктур при якому шляхом автоматизації процесу аналізування та керування ризиками досягається підвищення рівня автоматизації аналізування та керування ризиками, надійність захисту інформаційної інфраструктури, зниження вимог до кваліфікації фахівців, що зменшує загальну трудомісткість процесу аналізування та керування ризиками.

Поставлена задача вирішується тим, що у способі захисту інформаційних інфраструктур, при якому системно аналізують та керують ризиками застосовуючи центральний процесор та периферійну мережу приладів згідно з корисною моделлю додатково автоматизують аналізування та керування периферійною мережею приладів, яке виконує центральний процесор шляхом сканування її роботи, приймання інформаційних сигналів від неї, порівняння цих сигналів із вибраним еталоном, формування та передавання на периферійну мережу приладів керівних інформаційних сигналів для забезпечення автоматизованого захисту інформаційних інфраструктур, при цьому цю автоматизовану систему як невід'ємну частину інформаційних інфраструктур використовують протягом усього життєвого циклу діяльності цих інформаційних інфраструктур.

Метою запропонованого винаходу є створення корисної моделі - способу захисту інформаційних інфраструктур за допомогою аналізування та управління ризиків шляхом автоматизації усього життєвого циклу інформаційних інфраструктур починаючи з процесу їх інвентаризації, в тому числі і автоматизованої (Microsoft Systems Management Server 2003) яка задовольняє вимоги міжнародних стандартів в галузі захисту інформації та управління технічною інфраструктурою. Такий спосіб дозволяє за допомогою використання засобів інформаційних інфраструктур та відповідного програмного продукту автоматизовано проводити аналізування та управління ризиками, при цьому,

захист інформаційних інфраструктур стає більш надійним, з'являється можливість аналізування та управління ризиками в режимі реального часу, а виконувати аналізування та управління запропонованим способом може фахівець із середнім рівнем підготовки в сфері ІТ, навіть при відсутності досвіду в галузі захисту інформації. Крім цього, в запропонованому режимі автоматизації значно скорочується час на аналізування та управління ризиками за рахунок відсутності необхідності введення з боку оператора будь яких додаткових даних, окрім інформації, яка стосується складових елементів інформаційної інфраструктури та інформації щодо важливості її складових в процесі життєдіяльності загальної системи. При цьому, автоматизоване аналізування та управління ризиками як невід'ємна частина інформаційної інфраструктури, використовується протягом усього циклу її життєдіяльності. Запропонований спосіб розширює можливості застосування автоматизації способів аналізування та управління інформаційними інфраструктурами та надає можливість застосування таких технологій для виконання функцій, які не впливають з відомих раніше, що властиві цим технологіям, використання цих технологій з ціллю вирішення технічної задачі забезпечення автоматизованого захисту інформаційних інфраструктур шляхом автоматизованого аналізування та управління їх ризиками.

В основу корисної моделі поставлена задача захисту інформаційних інфраструктур із застосуванням процесу аналізування та управління ризиками шляхом автоматизації цього процесу протягом усього життєвого циклу інформаційних інфраструктур. Інформаційні інфраструктури з використанням процесу аналізування та управління ризиками дозволяють провести автоматизацію на всіх етапах діяльності інформаційних інфраструктур: від моменту створення інформації (інформаційних ресурсів, активів) до її знищення, включаючи етапи розповсюдження, зберігання, копіювання, передачі тощо.

Передові світові міжнародні стандарти в області інформаційної безпеки вимагають для ефективного управління безпекою інформаційних систем і інфраструктур обов'язкового впровадження аналізування та управління ризиками. При цьому можливо використовувати будь-які інструменти, завдяки яким є чітке розуміння того, що система інформаційної безпеки створена на основі аналізування ризиків, перевірена, керована та обґрунтована. Аналізування та управління інформаційними ризиками - ключовий фактор для побудови ефективного захисту будь яких інформаційних систем та інформаційних інфраструктур в цілому.

В компаніях, які досягли відповідного ступеню зрілості, проведення аналізування ризиків та управління ними на усіх стадіях життєвого циклу інформаційних інфраструктур є обов'язковим елементом у системі заходів щодо забезпечення режиму інформаційної безпеки. Вимоги до проведення цих етапів є різними, тому і технології аналізування ризиків є різними. Розробка методологій та методик аналізування ризиками пов'язана з рядом методологічних труднощів. Найбільша

складність полягає в розробці коректних процедур вимірювання ризиків та побудова моделі інформаційних інфраструктур з системних позицій, що враховують різнопланові фактори, які відносяться до організаційного, процедурного, програмно-технічного рівня та їх взаємних зв'язків.

Об'єктивно провести оцінювання якості методик, що використовуються для аналізування ризиків, допомагає ряд національних та міжнародних стандартів: BS 7799-3 Information security management systems. Guidelines for information security risk management (Руководство по управлению рисками информационной безопасности) (www.iso.org/iso), FIPS PUB 199 Standards for Security Categorization of Federal Information Systems (<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>), NIST Special Publication 800-60 (<http://csrc.nist.gov/publications/PubsSPs.html>) NIST Special Publication 800-30 (<http://csrc.nist.gov/publications/PubsSPs.html>).

Згідно з теорією безпеки пропонується використовувати абстрактні методи аналізування ризиків, а при переході до практичного застосування необхідно виконувати принципи і рекомендації по управлінню ризиками, що представлені в стандарті BS 7799-3.

Керівництво інформаційних служб та підрозділів розуміють необхідність приймати до уваги вимоги інформаційної безпеки, але при цьому ідуть по шляху впровадження інформаційних підсистем без загальної концепції захисту інформаційних ресурсів (активів).

Запропоноване рішення захисту інформаційних інфраструктур дозволяє впровадити автоматизований засіб інформаційного захисту, що в свою чергу дозволяє розробити загальну концепцію інформаційної безпеки, включаючи етап управління ризиками, який є наступним етапом після аналізування (оцінювання) ризиків у життєвому циклі інформаційних інфраструктур. Процеси аналізування (оцінювання) ризиків та управління ними є взаємопов'язаними. Вони вирішують задачу забезпечення захисту інформаційних інфраструктур послідовно та обов'язково застосовуються разом. При впровадженні запропонованого способу захисту інформаційних інфраструктур отримують додатковий ефект - ефект більш надійного та оперативного захисту від стороннього втручання, забезпечення персоналізації, посилення відповідальності посадових осіб, можливості простеження випадків порушення вимог безпеки.

Для реалізації способу використовують наступне обладнання - інформаційні інфраструктури:

- периферійні прилади (по меншій мірі два);
- датчики роботи периферійних приладів (по меншій мірі один для кожного приладу);
- сукупність периферійних приладів пов'язують мережею передачі даних з центральним процесором, який виконує аналізування та керування ризиками.

Роботу вищезазначеного обладнання автоматизують наступним чином:

- центральний процесор сканує роботу периферійних приладів;

- у відповідь на таке сканування, периферійні прилади передають інформаційні сигнали до центрального процесору;

- центральний процесор приймає ці інформаційні сигнали та автоматично порівнює їх із вибраним в якості еталону даними, при цьому проводить їх оцінювання відносно цього еталону;

- центральний процесор автоматично видає сигнал, який керує роботою периферійних приладів.

Таким чином здійснюють автоматичне керування периферійними приладами: сканування роботи периферійних приладів приймання та оцінювання систем роботи цих приладів відносно еталону, який встановлюють для порівняння із даними цих приладів.

Такі дані від периферійних приладів можуть, наприклад, оперативно вказувати на «взламвання» інформаційних інфраструктур, при цьому, також в оперативному режимі автоматично проводять керування такими системами: наприклад, при порушенні встановленого захисту, при аналізуванні інформаційних сигналів від периферійних приладів, центральний процесор блокує роботу усієї інформаційної інфраструктури.

Запропоноване рішення є новим та може бути промислово застосованим, запропонована система застосування автоматизованих інформаційних технологій може бути реалізована промисловим способом, оскільки її складові вузли і блоки побудовані на основі елементної бази широкого застосування.

Сукупність суттєвих ознак винаходу - корисної моделі, що заявляється, не відома з рівня техніки та може бути застосована в таких сферах, як інформаційні технології, а також використана в організаціях будь якої форми власності, комерційних структурах, транснаціональних компаніях тощо.

Таким чином, сукупність суттєвих ознак винаходу - корисної моделі, що заявляється, дозволяє застосувати спосіб захисту інформаційних інфраструктур шляхом автоматизації системи аналізування (оцінювання) та управління ризиками, при цьому, автоматизоване аналізування (оцінювання) та управління ризиками є невід'ємною частиною інформаційної інфраструктури яке використовується протягом усього її життєвого циклу.

Сутність запропонованої корисної моделі пояснюється наступними прикладами:

Приклад №1:

У фахівця в галузі IT-технологій (далі - користувача) є задача проведення автоматизованого оцінювання та впровадження дій по мінімізації інформаційних ризиків на всіх етапах життєдіяльності інформаційно-телекомунікаційної системи (інформаційної інфраструктури).

На першому етапі аналізування (оцінювання) та управління ризиками користувач проводить оцінювання ресурсу. Першим кроком оцінювання є ідентифікація всіх ресурсів інформаційної інфраструктури за допомогою способу будь якої глибини автоматизації, включаючи засіб Microsoft Systems Management Server 2003 та інші.

В результаті ідентифікації користувач вводить в автоматизовану систему аналізування (оціню-

вання) та управління ризиками (далі - автоматизованої системи) набір вхідних шаблонних даних визначених експертом-розробником автоматизованої системи, та необхідних системі для подальшого виконання процесу оцінювання та управління ризиками.

Наступним кроком є визначення та фіксація користувачем, в шаблонних формах автоматизованої системи, рівня доступності, конфіденційності, цілісності та важливості складових оцінюваної інформаційної інфраструктури. При цьому, користувач, який проводить оцінювання, повинен об'єктивно визначити зазначені рівні, базуючись на власному досвіді та досвіді відповідальних за ресурс фахівців.

Результатом цього етапу є формування автоматизованою системою узагальненого значення оцінки системи. Ці дії проводяться в автоматичному режимі, без участі користувача.

Наступним етапом в роботі автоматизованої системи по аналізуванню (оцінюванні) та управлінню ризиками є визначення з всієї множини загроз, уразливостей та існуючих засобів захисту актуальних для частини інформаційно-телекомунікаційної системи та розрахунок вірогідності їх реалізації. Актуальність баз загроз, уразливостей та існуючих засобів захисту в автоматизованій системі підтримує експерт-розробник автоматизованої системи.

Всі дії на цьому етапі проводяться в автоматичному режимі, без участі користувача.

Наступним етапом в роботі автоматизованої системи по аналізуванню (оцінюванню) та управлінню ризиками є визначення кількісної оцінки ризиків, як множини оцінки ресурсу та вірогідності реалізації загроз для кожного її виду.

Всі дії на цьому етапі проводяться в автоматичному режимі, без участі користувача.

Наступним етапом в роботі автоматизованої системи по аналізуванню (оцінюванню) та управлінню ризиками є процес управління ризиками на базі згенерованого за певним шаблоном автоматизованою системою звіту.

На базі звіту, користувач проводить процес управління ризиками - їх прийняття, передачу, зменшення або виключення.

Відповідальність за адекватне прийняття ризиків несе користувач.

Після прийняття рішення по управлінню, користувач вносить зміни в окремі позиції шаблону ідентифікації ресурсу і отримує оновленні данні щодо існуючих в інформаційно-телекомунікаційній системі ризиків.

Таким чином, запропонована корисна модель застосування способу захисту інформаційних інфраструктур, що заявляється, є новим перспективним напрямом у сфері автоматизації інформаційних інфраструктур і інформаційно-телекомунікаційних систем та може знайти широке застосування на практиці.