**Тимошенко Андрій Олександрович. Синтез систем захисту інформації з використанням логіко-імовірнісних методів : Дис... канд. наук: 05.13.21 – 2003**

|  |  |
| --- | --- |
| |  | | --- | | Тимошенко А.О. Синтез систем захисту інформації з використанням логіко-імовірнісних методів.– Рукопис.  Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. Національний технічний університет України “Київський політехнічний інститут”, Київ, 2002.  Дисертація присвячена розробці сукупності моделей, методів і алгоритмів, що можуть бути застосовані для розв’язання задачі побудови системи захисту інформації, оброблюваної в інформаційній системі з відкритою архітектурою.  З використанням методів логіко-імовірнісного моделювання розроблено аналітичну модель захищеної інформаційної системи з відкритою архітектурою. Сформульовано задачу побудови оптимальної системи захисту інформації, оброблюваної в інформаційній системі з відкритою архітектурою. Розроблено обчислювальний алгоритм розв’язання задачі побудови оптимальної системи захисту інформації, оброблюваної в інформаційній системі з відкритою архітектурою, в якому використовується розроблена модель. Розроблено формалізовані методики застосування розробленого алгоритму для побудови систем захисту інформації, оброблюваної в інформаційних системах різної структури. Практичне застосування розроблених методик дало успішні результати і підтвердило ефективність їхнього використання. | |
| |  | | --- | | У результаті виконання дисертаційної роботи отримані наступні результати:   1. Сформульовано задачу розробки і практичної реалізації сукупності моделей, методів і алгоритмів, що можуть бути застосовані для розв’язання задачі побудови системи захисту інформації, оброблюваної в ІС з відкритою архітектурою. На основі аналізу показано, що при розв’язанні задачі побудови СЗІ ІС повинна розглядатися як функціонуюча в умовах ризику, при невідомих законах і числових характеристиках розподілу спроб реалізації загроз інформації, а також потребуючих оцінки величинах потенційного збитку від реалізації різних загроз. Обґрунтовано можливість і виконано постановку задачі розробки, з використанням ЛІМ, моделі захищеної ІС з відкритою архітектурою. Виконано постановку задачі побудови оптимальної СЗІ з урахуванням обмежень на сумарну вартість засобів захисту. 2. Досліджено особливості ІС з відкритою архітектурою з погляду забезпечення захисту інформації, виявлено закономірності функціонування таких систем, яки необхідно врахувати в моделі, що розробляється: множина альтернативних шляхів розвитку НС при реалізації загроз інформації і ранжування показників значущості механізмів захисту, реалізованих на різних рівнях стека протоколів. З урахуванням виявлених закономірностей і умов функціонування ІС визначено структуру і набір параметрів моделі. Обґрунтовано можливість, на відміну від класичного ЛІМ, відображення в моделі множини загроз інформації не ймовірностями, а показниками ефективності реалізації, що характеризують ступінь ризику, пов'язаного з реалізацією загроз на різних рівнях стека протоколів 3. З використанням ЛІМ розроблено математичну модель захищеної ІС, що дозволяє оцінювати ймовірність збереження захищеності оброблюваної інформації при впливі на неї довільної множини загроз та відрізняється врахуванням умов і закономірностей функціонування ІС з відкритою архітектурою. 4. Розроблено алгоритм розв’язання задачі побудови оптимальної СЗІ з урахуванням обмежень на вартість засобів захисту на основі модифікованого градієнтного методу, у якому на кожній ітерації як напрямок руху приймається напрямок, що відповідає найбільшій питомій значущості за критерієм витрат і, для врахування закономірностей функціонування механізмів захисту, виконується відповідне коректування вектора змінюваних параметрів. Модифікація методу дозволила знизити обсяг обчислень більш ніж на 10%, а також знаходити рішення, що забезпечують більш ніж на 6% високу ймовірність збереження захищеності інформації. 5. Розроблено формалізовані методики визначення множини і характеристик загроз інформації та множини механізмів захисту, що включаються в модель захищеної ІС довільної структури, які базуються на результатах здійсненої класифікації відомих загроз інформації і типових механізмів захисту, результатах аналізу статистичних даних про інциденти з безпекою в розподілених обчислювальних мережах і розробленій ієрархії класифікаційних ознак загроз інформації. 6. Обґрунтовано і обрано принципи побудови і архітектуру програмного комплексу засобів автоматизації проектування СЗІ, що забезпечуює, за рахунок автоматизації основних етапів проектування, зниження витрат праці розробників у 2-5 разів. 7. Розроблені в дисертації моделі, методи і алгоритми були використані при створенні програмного комплексу засобів автоматизації проектування систем захисту інформації, оброблюваної в ІС з відкритою архітектурою. Даний комплекс засобів автоматизації впроваджений у навчальний процес у Фізико-технічному інституті НТУУ КПІ. Спроектовані з використанням розробленого комплексу системи захисту інформації впроваджені і успішно експлуатуються в ряді державних і комерційних установ України. | |