СИСТЕМИ ЗАХИСТУ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Ст. викладач М.А. Калінчук, студенти Е.А. Коновалов, М.Г. Костюк,
Дніпропетровський університет імені Альфреда Нобеля,
м. Дніпропетровськ

Нині стан захисту національних інформаційних ресурсів та систем викликає занепокоєність у всьому світі. Американські фахівці на основі наукових досліджень стверджують, що третя світова війна буде інформаційною. Або ж, якщо вона буде розв'язана, то врешті-решт кінцевий її результат визначить той, хто володіє стратегічно важливою інформацією. Тому питання захисту електронних платіжних систем є найважливішим при організації таких систем.

Можна виділити два підходи до забезпечення безпеки інформаційних систем:

1. *Фрагментарний* підхід орієнтується на протидію чітко визначеним загрозам при визначених умовах використання системи. Головною позитивною рисою такого підходу є міцний захист щодо конкретної загрози, але основний недолік – локальність дії та відсутність єдиного захищеного середовища для обробки інформації. Тому такий підхід неприйнятний для захисту платіжних систем.

2. Для створення захисту платіжних систем треба використовувати *комплексний* підхід, а саме: створення захищеного середовища для обробки платіжної та службової інформації в системі, яка об'єднує різноманітні (правові, організаційні, програмно-технічні) засоби для протидії будь-яким загрозам.

Створення надійної системи захисту можна розділити на чотири основних етапи: аналіз можливих загроз, розробка (планування) системи захисту, реалізація системи захисту, супроводження системи захисту під час експлуатації платіжної системи.

Всі загрози системи захисту для платіжної системи можна розподілити згідно з їхніми характеристиками, на класи: за цілями реалізації загрози; за принципом впливу на систему; за характером впливу на систему; за причинами появи помилок у системі захисту; за способом впливу на об'єкт атаки; за способом впливу на систему; за об'єктом атаки; за засобами атаки, що використовуються; за станом об'єкта атаки.