НАЦІОНАЛЬНА БЕЗПЕКА

Шишола І.М.
студент,
Навчально-науковий інститут захисту інформації
при Національній академії Служби безпеки України

ЗАБЕЗПЕЧЕННЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

У сучасному суспільстві значними темпами здійснюється впровадження новітніх досягнень комп'ютерних і телекомунікаційних технологій. Так, активно використовуються як локальні, так і регіональні обчислювальні мережі, значні території вже охоплені мережами мобільного зв'язку та інтернету. Наявні системи телекомунікацій активно впроваджуються у більшість галузей: промислові, торгові, юридичні, фінансові й соціальні галузі. Саме тому актуальною проблемо постає збереження й захист інформації.

Тривалий час методи захисту інформації розроблялися тільки державними органами, а їхнє впровадження розглядалося як виняткове право певної держави. Проте, зважаючи на збільшення спроб несанкціонованого доступу до конфіденційної інформації в останні роки, проблеми захисту інформації стали потребувати більшої уваги спеціалістів з різних країн світу.

На сьогодні інженерно-технічні заходи являють собою сукупність спеціальних органів, технічних засобів і заходів, що функціонують спільно для виконання певного завдання щодо захисту інформації. До інженерних засобів відносять екранування приміщень, організація сигналізації, охорона приміщень з ПК.

Технічні засоби захисту включають в себе апаратні, програмні, криптографічні засоби захисту, які ускладнюють можливість атаки, допомагають виявити факт її виникнення, позбутися від наслідків атаки.

Для реалізації зазначених функцій можуть використовуватися наступні механізми:

- шифрування, перетворює інформацію в форму, недоступну для розуміння неавторизованими користувачами;
- електронний цифровий підпис, що переносить властивості реальної підпису на електронні документи;
- механізми управління доступом, які керують процесом доступу до ресурсів користувачів на основі такої інформації як бази даних управління доступом, паролі, мітки безпеки, час доступу, маршрут доступу, тривалість доступу;
- механізми контролю цілісності, контролюючі цілісність як окремого повідомлення, так і потоку повідомлень і використовують для цього контрольні суми, спеціальні мітки, порядкові номери повідомлень, криптографічні методи;
- механізми доповнення трафіку, що додають в потік повідомлень додаткову інформацію, «що маскує» від зловмисника корисну інформацію;

- механізми ідентифікації, які на підставі пропонованих користувачем паролів, пристроїв, що здійснюють ідентифікацію або його біометричних параметрів приймають рішення про те, чи є користувач тим, за кого себе видає.

Технічні засоби підсистем безпеки сучасних розподілених інформаційних систем виконують такі основні функції:

- ідентифікація партнерів по взаємодії, що дозволяє переконатися в справжності партнера при встановленні з'єднання;
- ідентифікація джерела інформації, що дозволяє переконатися в справжності джерела повідомлення;
- управління доступом, що забезпечує захист від несанкціонованого використання ресурсів;
- конфіденційність даних, яка забезпечує захист від несанкціонованого отримання інформації;
- цілісність даних, що дозволяє виявити, а в деяких випадках і запобігти зміні інформації при її зберіганні і передачі;
- приналежність, яка забезпечує доказ приналежності інформації певній особі.

Потрібно розуміти, що з об'єктивних причин взагалі виключити загрози завданню шкоди базі інформаційних даних або несанкціонованому втручанню у них неможливо. Метою робіт з приводу захисту інформації повинен бути комплекс адміністративних, процедурних і програмно-апаратних заходів, спрямованих на мінімізацію витоку інформації через співробітників. Основна ідея всіх заходів (як для паперової, так і для електронної інформації) наступна: скоротити кількість людей, допущених до конкретної інформації до мінімально необхідного, суворо розмежовувати доступ до сховищ інформації, контролювати, хто отримав інформацію, захищати процес її передачі.

В свою чергу адміністративні та процедурні заходи захисту повинні структурувати і максимально формалізувати відносини між підрозділами, документальні потоки між ними, правила спілкування відділів, правила передачі інформації між ними. Тобто, основне завдання адміністративних заходів – обмежити коло осіб, що мають доступ до кожного виду інформації, зафіксувати тих, хто може мати до неї доступ, впорядкувати місця її зберігання (і електронної, і паперової), ввести правила поводження з конфіденційними документами. На таку структуровану систему вже досить просто накладати захисні механізми. На основі цього вже будуть формуватися політика безпеки і конфігурації, які закладаються в програмно-апаратні засоби захисту.

Узагальнюючи, слід зазначити, що проблема захисту комп'ютерної системи є частиною загальної проблеми інформаційної безпеки організації. Її вирішення найбільш ефективно тільки в комплексі організаційних і процедурних заходів щодо захисту інформації, які повинні підтримуватися єдиним комплексом програмно-технічних засобів захисту. Цей складний розвиває організм, який має складну внутрішню структуру, що діє за своїми власними законами, має своєю головною метою забезпечення безпеки організації, її інформації та інформаційних потоків.