УДК 004.056.53(043.2)

Максімов Ю.О.
Національний авіаційний університет, Київ

ЗАГРОЗИ ТА СПОСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МЕРЕЖЕВИХ РЕСУРСІВ

Вступ. Захист від несанкціонованого доступу до мережевих ресурсів інформаційних систем – один із головних елементів забезпечення цілісності передачі конфіденційної інформації. З активною інформатизацією сучасного суспільства загострюються проблеми надійності користування мережевими системами.

Актуальність. Щоденно зловмисники піддають загрозам мережеві інформаційні системи, намагаючись отримати до них доступ та контроль і використовуючи для цього спеціальні дії – атаки, які стають все більш витонченими за впливом і нескладними у виконанні.

Постановка завдання. Для надійного захисту систем, що використовують мережеві ресурси необхідно знати та чітко класифікувати загрози, що можуть бути вчинені зловмисниками, а також застосовувати ефективні способи боротьби.

Мета – провести аналіз існуючих загроз щодо мережевих ресурсів і виробити рекомендації щодо зменшення їх шкідливого впливу.

Найбільш поширеними атаками мережевих ресурсів є: підслуховування; перехоплення пароля; підміна довіреної адреси; посередництво; відмова в обслуговуванні; мережева розвідка; спам та фішинг.

Відповідно до різновидів атак слід застосовувати різноманітні технології захисту інформації у комплексному підході вирішення цього питання, такі як:

- ідентифікація і автентифікація користувачів;
- управління доступом та забезпечення централізованого управління;
- протоколювання і аудит;
- криптографія;
- екранування;
- забезпечення високої доступності.

Результати. Перераховані типи атак на IP-мережі можливі через ряд причин, серед яких: використання загальнодоступних каналів передачі даних; уразливості процесу ідентифікації; відсутність в стеці протоколів TCP/IP механізмів забезпечення конфіденційності та цілісності переданих повідомлень; аутентифікація здійснюється за IP-адресою, що надалі не перевіряється; відсутність можливості контролю за маршрутом проходження повідомлень, що робить віддалені мережеві атаки практично безпокараними.

Висновок. Вироблення чіткої і збалансованої політики безпеки та застосування засобів захисту на всіх рівнях корпоративної мережевої системи дозволяє забезпечити комплексний підхід до безпеки, орієнтований на створення захищеного та убезпеченого середовища обробки інформації в мережевих системах, що об'єднує в єдиний комплекс різнорідні заходи протидії загрозам.

Науковий керівник – О.В.Дубчак.