УДК 004.78 (043.2)

Семко О.
Національний авіаційний університет, Київ

КОМЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

Як відомо, під терміном «комплексна система захисту інформації» розуміють комплекс організаційних та інженерно-технічних заходів, направлених на забезпечення вимог захисту інформації в інформаційно-телекомунікаційній (автоматизованій) системі та спрямованих на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу , який включає організаційні і інженерно-технічні заходи.

Як відомо, одним з найбільш розповсюджених механізмів захисту є застосування міжмережевих екранів - брендмауерів (firewalls).

Міжмережевий екран виконує свої функції, контролюючи всі інформаційні потоки між інформаційно-телекомунікаційними системами, працюючи як деяка "інформаційна мембрана". У цьому сенсі міжмережевий екран можна уявити собі як набір фільтрів, що аналізує інформацію і на основі закладених у нього алгоритмів (правил), приймає рішення щодо пропуску чи відмові пропуску (відмові в обслуговуванні) інформації. Відповідно до цього існує інженерно-технічний засіб КСЗІ – міжмережеве екранування.

Іншими досить важливими інженерно-технічними заходами КСЗІ в Інтернеті є обмеження доступу в WWW серверах, обмеження за IP-адресами, обмеження за ідентифікаторами одержувача.

Суть останнього зводиться до того , що доступ до приватних документів можна дозволити, або навпаки заборонити використовуючи привласнене ім'я і пароль конкретному користувачу, причому пароль у явному вигляді ніде не зберігається.

Поряд із забезпеченням безпеки програмного середовища найважливішим буде питання про розмежування доступу до об'єктів Web-сервісу , тобто захист web-серверів. У Web-серверах об'єктами доступу виступають універсальні локатори ресурсів (URL - Uniform (Universal) Resource Locator). За цими локаторами можуть стояти різні сутності - HTML-файли, CGI-процедури і т.п.

Зрозуміло, захист системи, на якій функціонує Web-сервер, повинна випливати універсальним рекомендаціям, головне з яких є максимальне спрощення. Усі непотрібні сервіси, файли, пристрої повинні бути вилучені. Число користувачів, що мають прямий доступ до сервера, повинне бути зведене до мінімуму, а їхні привілеї - упорядковані у відповідності зі службовими обов'язками.

Науковий керівник – Є.Б. Артамонов, к.т.н.