УДК 004.056.53

В.В. Липявка,
Г.В. Мартинюк, к.т.н.
Національний авіаційний університет, Київ

ПОБУДОВА СИСТЕМИ ОХОРОННОЇ СИГНАЛІЗАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Завдання забезпечення інформаційної безпеки в сучасному світі є особливо актуальним. Це пов'язано з широким впровадженням комп'ютерних систем та мереж на різноманітних об'єктах інформаційної діяльності. Вони здобули широке використання у всіх галузях промисловості, фінансових операціях, обліку тощо.

Організаційні вимоги до системи захисту передбачають реалізацію сукупності адміністративних і процедурних заходів. Вимоги щодо забезпечення схоронності мають виконуватися, насамперед, на адміністративному рівні. Організаційні заходи, проведені з метою підвищення ефективності захисту інформації, повинні передбачати такі процедури:

-обмеження несупроводжуваного доступу до обчислювальної системи;

-здійснення контролю за зміною в системі програмного забезпечення, виконання тестування і верифікації змін у системі програмного забезпечення і програмах захисту;

-організація і підтримання взаємного контролю за виконанням правил захисту даних;

-обмеження привілею персоналу, що обслуговує ІС;

-здійснення запису протоколу про доступ до системи;

-гарантія компетентності обслуговуючого персоналу;

-розробка послідовного підходу до забезпечення схоронності інформації для всієї організації.

Підсистема керування доступом має забезпечувати: ідентифікацію, аутентифікацію і контроль за доступом користувачів (процесів) до системи, терміналів, вузлів мережі, каналів зв'язку, зовнішніх пристроях, програм, каталогів, файлів, записів і т.д.; керування потоками інформації, очищення областей, що звільняються, оперативної пам'яті і зовнішніх накопичувачів.

У роботі представлено модель загроз для інформації з обмеженим доступом, що циркулює на об'єкті інформаційної діяльності. Згідно

з представленою моделлю можна описати технічні канали витоки інформації та шляхи недопускання цього.

Акустичний канал може бути створений: шляхом безпосереднього прослуховування розмов; шляхом перехоплення мовних сигналів за допомогою портативних технічних засобів акустичної розвідки (диктофонів та магнітофонів); шляхом застосування МНД та акустичних антен, що встановлюються в зоні прямої видимості. Для захисту мовної інформації від витоку можна застосовувати різноманітні проектно-архітектурні рішення, а саме: зашумлення, звукоізоляцію або ж кімнати для ведення переговорів розташовувати в місцях, де зняття інформації унеможливлене архітектурою будівлі.

Візуально-оптичний канал. За допомогою зорової системи людина отримує найбільший (до 90%) обсяг інформації із зовнішнього світу. Інфрачервоний і ультрафіолетовий спектри також несуть істотну інформацію про навколишні предмети. З метою захисту інформації від витоку рекомендується: робити просторові огородження; ввести енергетичні обмеження; використовувати засоби загародження або значного ослаблення відбитого світла; застосовувати засоби маскування, імітації та інші з метою захисту та введення в оману зловмисника.

Витік інформації по ланцюгам заземлення. Так як кола заземлення виходять за межі приміщення і будівлі, то сигнали, які поширюються по ним можуть бути зняті за допомогою технічних засобів. Небезпечний сигнал може бути «знятий» з кола заземлення індуктивним способом або з опору, включеного послідовно в цей ланцюг.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Кулаков Ю. А., Луцкий Г. М. Компьютерные сети. – К.: Юниор, 1998. – 380 с.

2. Бэрри Нанс. Компьютерные сети / Пер. с англ. – К.: Бином, 1995. – 214 с.

3. Торокин А.А. Основы инженерно-технической защиты информации /А.А. Торокин. – М.: Ось-89, 1998. – 336с.

4. Каторин Ю.Ф. Большая энциклопедия промышленного шпионажа /Ю.Ф. Каторин и др. – СПб.: Полигон, 2000. – 896с.