

УДК 004.056.5

ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ ОСНОВИ МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

К.Л. Шевченко, доктор технічних наук, професор
Національний Технічний університет України «КПІ» ім. Сікорського»

А.С. Андреев, магістрант

Київський національний університет технологій та дизайну

Ключові слова: захист інформації, метрологічне забезпечення, система контролю, похибки вимірювань.

Сьогодні питання технічного захисту інформації є дуже важливим, оскільки стрімкий розвиток сучасних технологій потребує усе більшої надійності приладів для забезпечення зберігання інформації, запобігання її обробки, зчитування чи спотворення сторонніми особами.

Відповідно до чинного законодавства України обов'язковому захисту підлягає інформація, що є власністю держави, або інформація з обмеженим доступом, вимоги по захисту якої встановлені законодавством, в т.ч. персональні дані громадян.

Забезпечується це комплексними системами захисту інформації, що передбачають використання сукупності організаційних і технічних заходів.

До організаційних заходів відносять створення концепції інформаційної безпеки, зокрема:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;
- розробку планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів або виникнення надзвичайної ситуації;
- навчання користувачів правилам інформаційної безпеки.

До технічних заходів відносять використання сукупності спеціальних технічних засобів та їх використання для захисту інформації. Вибір технічних засобів залежить від вимог до рівня захищеності інформації.

Відповідно до рекомендацій [1], найбільш розповсюдженими потенційно небезпечними з точки зору захисту інформації вважаються:

- засоби і системи телефонного, телеграфного (телетайпного), директорського, гучномовного, диспетчерського, внутрішнього, службового та технологічного зв'язку;
- засоби і системи звукопідсилення, звукозапису та звуковідтворення;
- пристрої, що утворюють дискретні канали зв'язку: абонентська апаратура із засобами відображення та сигналізації, апаратура підвищення достовірності пересилання, каналоутворювальна тощо;

- апаратура перетворення, оброблення, пересилання і приймання відеоканалів, що містять факсимільну інформацію.

Інформація, що передається наведеними вище засобами, може зніматися за допомогою різних каналів, як показано на рис.1.



Рисунок 1- Структура технічних каналів витоку інформації

Технічний канал витоку можна вважати захищеним, якщо сигнал не перевищує встановленого нормативною документацією відношення "інформативний сигнал/шум".

Прилади, які забезпечують захист інформації та визначають придатність об'єкту до використання згідно чинних в Україні нормативних документів та повірочних схем та процедур, мають проходити:

- державні метрологічні випробування;
- метрологічну атестацію;
- повірку;
- калібрування.

На даний момент в Україні існує 37 затверджених повірочних схем, які можна використовувати задля метрологічного забезпечення якості приладів у сфері технічного захисту інформації. Аналіз повірочних схем показує, що в багатьох випадках вони не забезпечені еталонами, або прецизійними засобами вимірювання [2]. Тому першочерговим завданням технічної складової систем захисту інформації є забезпечення високоточними засобами вимірюваннями в акустичному, електромагнітному та оптичному каналах.

Список використаних джерел

1. Нормативний документ системи технічного захисту інформації

(ТР ЕОТ-95) – Режим доступу:

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=120206&cat_id=89769&ctime=1421836194327.

2. Юзьків Я. Нормативне та метрологічне забезпечення захисту інформації / Я. Юзьків, Є. Козир, О. Шевченко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник. – 2000. – № 1. – С. 94-99.