Завдання №19

Захист ОІД. Методи захисту;

Категоріювання норм (на первинні параметри):

У залежності від умов розташування об’єктів встановлені категорії норм за визначеними для кожного виду технічних засобів (ТЗ) каналах витоку інформації:

1 категорія – встановлюється для об’єктів інформаційної діяльності (ОІД) де циркулює інформація що складає відомості з грифом (ОВ);

2 категорія – встановлюється для об’єктів інформаційної діяльності (ОІД) де циркулює інформація що складає відомості з грифом (ЦТ);

3 категорія – встановлюється для об’єктів інформаційної діяльності (ОІД) де циркулює інформація що складає «таємні» відомості.

Причому до таємної інформації відноситься інформація, котра складає державну чи іншу передбачену Законом таємницю, та доступ до неї громадян здійснюється згідно з Законом про цю інформацію за ступенями секретності („особливої важливості”, „цілком таємно”, „таємно”).

В узагальненій моделі загроз, ТР розглядається як система перехоплення, котра у відношенні до об’єктів різних категорій має такі оперативно-технічні можливості:

- ТР діє на межі КЗ;

- ТР залучає для перехоплення ІС оптимальні або квазиоптимальні приймачі;

- ТР веде перехоплення по будь-якому з паразитних КВ;

- для ОІД I та II категорій перехоплення може вестись безперервно, без обмежень часу, з можливим накопиченням даних та залученням ТР всіх видів апріорної інформації про сигнали, апаратуру і т.п.;

- для ОІД III категорії час перехоплення обмежений, моменти перехоплення більш чи менш випадкові, ТР практично не має апріорної інформації про сигнали і завади.

Завади, котрі враховуються при визначенні захищеності інформації від витоку, повинні задовільняти слідуючим вимогам: - маскуючі властивості завад повинні зберігатись на заданому рівні при використанні будь-яким з методів обробки суміші сигнал-завада. Інакше кажучи, властивості завад повинні бути стабільними в часі і в просторі. Завади, котрі діють у КВ інформації, як витікає з выщезазначеного, складаються з багатьох компонент з різним ступенем детермінованості, з різними розподіленнями потужності по частоті і стабільністю рівня в часі і просторі. На основі аналізу зазначених джерел завад та вимог до них і розроблюються методики визначення рівнів завад в КВ інформації. За допомогою зазначених методик провадять виміри.

Використання мінімальних значнь завад гарантує ефективний захист інформації від витоку незалежно від розміщення об’єктів.

Ідеологія та приклади реалізації інформаційної атаки з використанням ВЧ нав’язування;

Ідеологія

Технічний канал витоку інформації шляхом ВЧ нав’язування можна забезпечити шляхом несанкціонованого контактного введення току ВЧ від генератора, підключеного до лінії (кола), що має функціональний зв’язок з нелінійним чи параметричним елементом ДТЗС, на котрих здійснюється модуляція ВЧ сигналу інформаційним. Інформаційний сигнал в даних елементах ДТЗС з’являється як слідство електроакустичного перетворення акустичних

сигналів в електричні. Згідно тому, що нелінійні або параметричні елементи ДТЗС для ВЧ сигналу, як правило, являють собою неузгоджене навантаження, промодульований ВЧ сигнал буде відбиватися від неї та поширюватись в зворотному напрямку по лінії, або випромінюватись. Для прийому випромінених або відбитих ВЧ сигналів використовуються спеціальні приймачі з високою чутливістю.

Приклад

Для зняття акустичної інформації з закритого приміщення дедалі частіше використовується так зване ВЧ-нав’язування, коли для зняття інформації використовується будь-який “цінний” подарунок (наприклад, картина або естамп), виконаний так, що він стає резонансним елементом модуляційної системи. При ВЧ опромінюванні цього елементу відбувається модуляція мовними сигналами спрямованого на цей елемент високочастотного радіовипромінювання. Таким самим чином, розрахувавши або експериментально з’ясувавши резонансні характеристики дзвінкового кола телефонного апарату чи, наприклад, трансформаторного кола радіоточки, можна зняти мовну інформацію за допомогою ВЧ-нав’язування

Активні засоби. Постановка завад. Види завадових сигналів. Приклади приладів та їх характеристики;

Активні методи захисту спрямовані на:

- створення просторових маскуючих електромагнітних завад з ціллю зменшення відношення сигнал/завада на межі зони що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

- створення маскуючих електромагнітних завад у сторонніх провідниках та з’єднувальних лініях ДТЗС з ціллю зменшення відношення сигнал/завада на межі зони що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

Ослаблення побічних електромагнітних випромінювань ТЗПІ та їх наведень у сторонні провідники здійснюється шляхом екранування та заземлення ТЗПІ та їх ліній заземлення.

Послаблення просочування інформаційних сигналів ТЗПІ до мереж електроживлення здійснюється шляхом фільтрації інформаційних сигналів.

Відрізняють такі способи екранування:

- електростатичне екранування;

- магнітностатичне екранування;

- електромагнітне екранування

Види сигналів заваових

Метод синфазної НЧ маскуючої завади

Метод ВЧ маскуючої завади

Метод ультразвукової Маскуючої завади

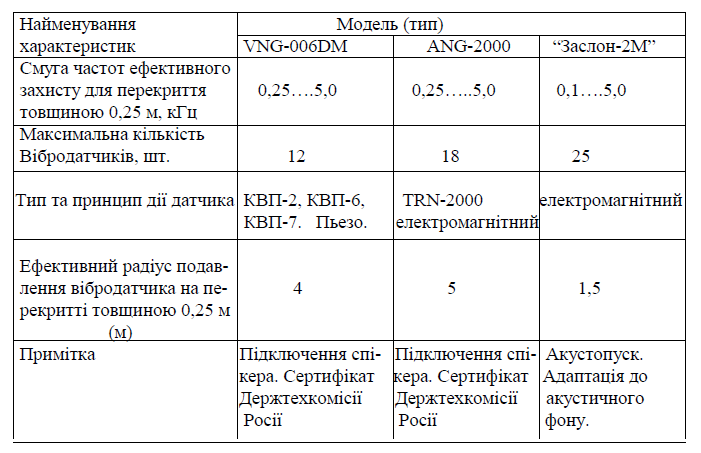
Метод підвищення напруги

Метод “понулення”

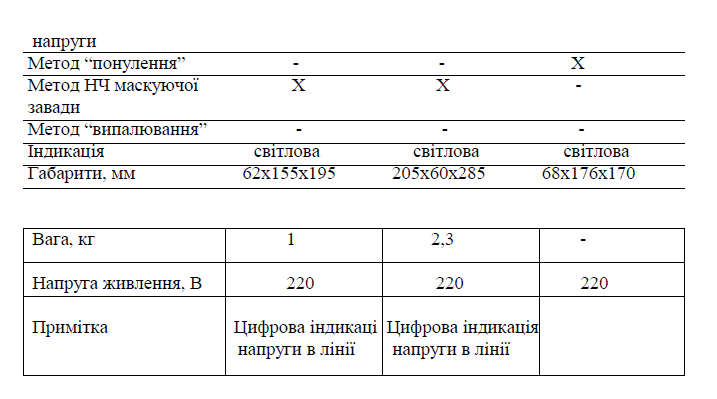
Метод “випалювання”

Метод НЧ маскуючої завади

Приклади приладів







Методи і засоби виявлення та знешкодження диктофонів.

\*знешкодження закладних пристроїв:

- знешкодження закладних пристроїв, що підключені до лінії, з використанням спеціальних генераторів імпульсів (випалювачів “жучків”).

Виявлення закладних пристроїв здійснюється проведенням спеціальних досліджень та спеціальних перевірок об’єктів ТЗПІ та виділених приміщень.

Спеціальні дослідження виділених приміщень та об’єктів ТЗПІ провадяться шляхом іх візуального огляду без залучення технічних засобів.

Спеціальна перевірка провадиться з використанням технічних засобів. При цьому здійснюється:

\*виявлення закладних пристроїв з використанням пасивних засобів:

- встановлення засобів і систем виявлення лазерного випромінювання (підсвітлення) віконних стекол;

- встановлення стаціонарних виявителів диктофонів;

- розшук закладних пристроїв з використанням індикаторів поля, інтерсепторів, частотомірів, скануючих приймачів та програмно-апаратних комплексів контролю.

- організація радіоконтролю (постійно, або на час проведення конфіденційних заходів) і побічних електромагнітних випромінювань ТЗПІ.

\*виявлення закладних пристроїв з використанням активних засобів:

- спеціальна перевірка виділених приміщень з використанням нелінійних локаторів;

- спеціальна перевірка виділених приміщень, ТЗПІ та допоміжних технічних засобів з використанням рентгенівських комплексів.