

ЛАБОРАТОРНИЙ СТЕНД ДЛЯ СТВОРЕННЯ ІМІТАТОРІВ ЗАКЛАДНИХ ПРИСТРОЇВ

Іванишин Денис Дмитрович, Кручинін Олександр Володимирович
Національний гірничий університет, nmu.org.ua, D.Ivanyshyn@tech-center.com

Висвітлена проблема підготовки спеціалістів в сфері технічного захисту інформації. Запропоновано підхід щодо вдосконалення принципів будови, структури та особливостей закладних пристроїв.

Ключові слова – закладний пристрій; імітатор; підготовка спеціалістів.

ВСТУП

Ефективна організація обміну інформацією набуває дедалі більшого значення як обов'язкова складова успішної практичної діяльності сучасного соціуму. Відповідно в умовах сьогодення надзвичайно актуальним є вдосконалення систем інформаційного забезпечення.

Інтенсифікація інформаційних процесів створює суттєві проблеми, без розв'язання яких не можна досягти ефективності інформатизації. Однією із найбільш гострих нині є проблема захисту інформації. Процеси, з допомогою яких забезпечується попередження та нейтралізація загроз для інформації, включає також технічний захист інформації (далі – ТЗІ) – діяльність, спрямовану на забезпечення інженерно-технічними засобами порядку доступу, цілісності й доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності й доступності відкритих відомостей, важливих для особи, суспільства і держави.

Питання, що являються складовими частинами ТЗІ, є досить складними технічно, адже включають в себе широкий спектр як загальних сфер знань: математика, фізика, комп'ютерні мережі, радіоелектроніка, теорія зв'язку, так і спеціальні: криптографія, стеганографія, методи та засоби захисту інформації. Через це, спеціалісти даної сфери потребують специфічної підготовки, яка включає в себе знання теоретичної бази, так і практичні навички.

ЛАБОРАТОРНИЙ СТЕНД ДЛЯ ВИВЧЕННЯ БУДОВИ ЗП

Складність, при підготовці інженерів з ТЗІ, має саме практична частина, адже, з одного боку, така діяльність є не стандартною в організаційному плані, а з іншого потребую специфічного обладнання, яке, найчастіше, є занадто дорогим, не доступним, не випускається взагалі або дрібними серіями. Прикладом такого обладнання є апаратура, яка необхідна для вивчення розділу про захист інформації від витоку за рахунок закладних пристроїв.

Для забезпечення високого рівня підготовки спеціаліста, він повинен володіти навичками виявлення і локалізації закладних пристроїв (ЗП). Першочерговим, для досягнення цієї цілі, є досконале володіння прийомами роботи з спецприладами, але, крім цього, дуже важливим є ознайомлення з принципами і особливостями роботи «закладок». Ця задача є неймовірно складною, адже на сьогодні існує різноманіття цих пристроїв. Перші «закладки» були аналоговими, використовували амплітудну, або частотну модуляцію, і передавали сигнал в постійному режимі. Після них з'явилися пристрої з системою голосового керування (передача починалася лише при наявності звукових сигналів певного рівня), пізніше, для ускладнення виявлення сигналів технічного засобу несанкціонованого зйому інформації використовувалась псевдовипадкова перестройка несучої частоти. А далі настала ера цифрових закладних пристроїв, які дали змогу реалізувати передачу інформації в імпульсному режимі, з проміжним накопиченням, дистанційно керовані пристрої. В джерелах (1) є досить повна класифікація ЗП.

На сьогодні на ринку представлений широкий вибір імітаторів закладних пристроїв, наприклад «Шиповник-1», «Шиповник-2», «Аврора», «ІМФ-2», «Імпульс» та ін. В них реалізовані демаскуючі ознаки вище згаданих «закладок». Основною їх задачею є перевірка працездатності пошукових приладів, з чим і пов'язані їх конструктивні особливості: розміщені вони в габаритних корпусах, з індикацією режимів роботи та їх перемикачами. Як результат, вони є непридатними для використання при навчанні пошуку закладних пристроїв студентів, так як їх таємне встановлення ускладнене. Також важливими характеристиками приладів, залучених в навчальному процесі, є їх ремонтпридатність і стійкість до фізичних впливів, адже в процесі роботи, не виключена можливість необережного поводження з ними, яка призведе до виходу імітатора із ладу. Крім того при використанні пристроїв заводського виготовлення їх схемо-технічні особливості залишаться недоступними для студентів, що призведе до не достатнього розуміння процесів і принципів, що лежать в основі роботи закладних пристроїв. Таким чином виявлено ряд недоліків, які вказують на невисоку доцільність використання зразків імітаторів закладних пристроїв доступних на ринку.

Виходячи з вищевказаних фактів доцільним є, створення універсального імітатора, складовими частинами якого б були модулі, різні комбінації яких дозволили б створити практично будь-який закладний пристрій, відомий сьогодні. Найбільш поширеними на сьогодні є акустичні «закладками», тому серед

модулів необхідними є блок формування сигналів мікрофону, підсилювачів низької частоти різної складності. Для реалізації апаратних закладок необхідним є модуль формування цифрових сигналів, телефонних – адаптер під'єднання до телефонної лінії. Імітація приладу не санкціонованого зйому видової інформації можлива з реалізацією блоку формування відеосигналу. Створення цифрової закладки потребує модулів аналогово-цифрового перетворення, керування. Можливість зовнішнього керування закладкою потребує встановлення блоку трансивера. Реалізація пристрою з накопиченням сигналу вимагає наявності елементів проміжного зберігання інформації. Імітатор закладки з передачею по радіоканалу має в своєму складі модуль формування ВЧ сигналів, інфрачервоному – модуль формування ІЧ сигналів.

Одже, на даний момент до складу приладу планується включити наступні модулі:

- формування сигналів мікрофону;
- генератора цифрових сигналів;
- формування відеосигналу;
- адаптеру під'єднання до телефонної лінії;
- підсилювача низької частоти;
- підсилювача низької частоти з автоматичним;

- регулюванням підсилення;
- аналогово-цифрового перетворення;
- проміжного накопичення сигналу;
- блоку керування;
- трансиверу;
- формування сигналів ВЧ ;
- формування сигналів ВЧ з кварцовою стабілізацією;
- інфрачервоної передачі;

Запропоновані модулі складуть основу навчального комплексу для вивчення принципів роботи ЗП.

ВИСНОВОК

З реалізацією даного лабораторного стенду підготовка спеціалістів, в розглянутій сфері, дозволить забезпечити новий якісний рівень.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Хоррев А. А. Защита информации от утечки по техническим каналам. М.:1997.
2. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. Юниор : 2003
3. analitika.info Каталог средств безопасности: имитаторы закладных устройств.