Прилади для виявлення закладних пристороїв

Пошуковий комплекс “Delta-X”

Швидко і надійно виявляє всі види мобільних пристроїв котрі знімають інформацію, включаючи аналогові, цифрові, що працюють постійно і періодично, передають аудіо або відео, з шифруванням або без нього.

Знаходить підслуховуючі пристрої, що використовують цифрові стандарти GSM, 3G, 4G / LTE, Bluetooth, Wi-Fi, DECT і т.д.

Нелінійний локатор “Лорнет 24”

Лорнет-24 використовується при проведенні оперативно-пошукових робіт в приміщеннях, в автомашинах, огляді людей і бандеролей, виявляє технічні засоби і пристрої, що мають в своєму складі напівпровідникові компоненти. Оснащений системою автоматичного вибору частот і може автоматично відбудовуватися від зосереджених перешкод (за критерієм мінімального шуму в каналі прийому 2-ї гармоніки).

Сканер безпровідних відеокамер “C-Hunter”

C-Hunter 935B - нова модель сканера бездротових відеокамер. Швидкість сканування всього частотного діапазону не перевищує 20 секунд, завдяки чому прихований відеопередавач досить швидко виявляється, після чого сканер налаштовується на його частоту і включається перехоплення зображення з нього.

Виявляч прихованих відеокамер “Wega”

Унікальний мініатюрний пристрій було створено професіоналами технічних засобів захисту інформації для надійного і швидкого виявлення прихованих відеокамер. В основі роботи детектора лежить оптичне зондування, яке дозволяє проводити вдале виявлення мікрооб'єктива прихованих фото і відеокамер по їхніми оптичним ознаками залежно від робочого стану каналу передачі і об'єкта відеосигналу.

Багатофункціональний пошуковий прилад “Піранья ST 031”

ST-031 «Піранья» призначений для проведення оперативних заходів по виявленню та локалізації технічних засобів нелегального отримання інформації, а також для виявлення і контролю природних і штучно створених каналів витоку інформації. Хороший пошуковий комплекс з великим функціоналом.

Аналізатор ліній “ULAN-2”

Прилад "УЛАН-2" (п'яте покоління) призначений для виявлення фактів несанкціонованого підключення до різних провідних комунікацій, таких як телефонні лінії, електричні мережі змінного струму, комп'ютерні мережі, лінії охоронної сигналізації і т.д.

Індикатор поля “I-protect”

iProtect 1205 - простий і високоефективний пристрій. У своїй схемі містить сучасні високо технологічні елементи, що дозволяє оператору проводити пошукові роботи на високому професійному рівні. Перевага РЧ детектора - широкий діапазон частот і здатність виявляти і локалізувати джерела радіовипромінювання і, отже, показувати місце розташування передавача.

Прилади для виявлення побічних електромагнітних випромінювань та наведень

Аналізатор спектру “Egilent N1996A”

Аналізатор спектру Agilent CSA виходить на такий рівень технічних характеристик, який і не можна було собі уявити в компактному аналізаторі спектру. Найширший динамічний діапазон для такого цінового класу приладів досягнутий завдяки незрівнянно низькому рівню спотворень, істотному поліпшенню шумових характеристик і наявності в стандартній комплектації приладу смуги пропускання 10 Гц.

Електрична вимірювальна антена “АИ-5.0”

АІ 5-0 призначена для вимірювання побічних електромагнітних випромінювань і наведень (ПЕМВН) від різних радіоелектронних пристроїв (РЕП) і застосовується в сфері оборони і безпеки, а також при проведенні робіт із забезпечення електромагнітної сумісності РЕП. Забезпечує високу точність вимірювання на малих відстанях від досліджуваних РЕП. Використовується як в закритих приміщеннях (лабораторії, екрановані камери і т.д.), так і на відкритій площі.

Магнітна вимірювальна антена “ММА-30”

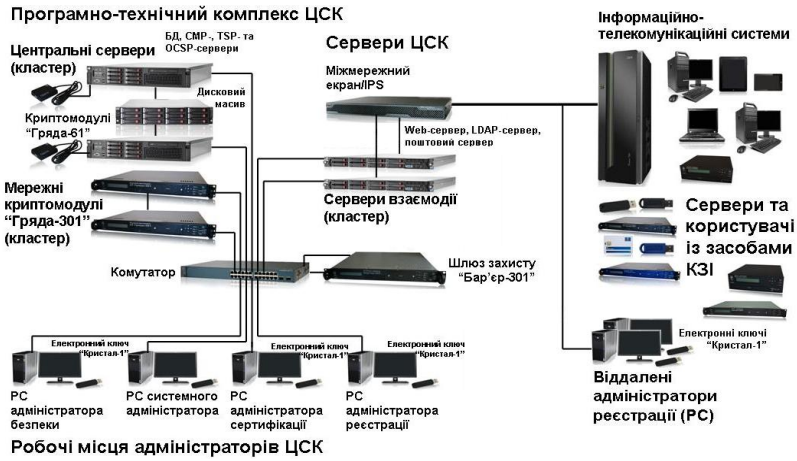
Призначення даної антени: вимір напруги по магнітній складовій поля в діапазоні 0.009-40 МГц.

Прилади для виявлення акустичного та віброакустичного каналу

Шумомір-Віброметр “Екотензор-110А”

Даний шумомір має пряме підключення мікрофонів і вібродатчиків, може одночасно вимірювати шум і трикомпонентні вібрації, одночасно вимірює звук і повітряний ультразвук, також вимірює звук та інфразвук, вимірює вібрації одночасно в чотирьох точках в діапазоні частот до 10 кГц.

Центр сертифікації ключів



Програмно-технічний комплекс центру сертифікації ключів (ЦСК) призначений для реалізації регламентних процедур та механізмів обслуговування сертифікатів відкритих ключів користувачів центру, надання послуг фіксування часу, надання користувачам засобів електронного цифрового підпису (ЕЦП) та шифрування, а також засобів генерації особистих та відкритих ключів.

Технічні засоби комплексу об’єднані у локальну обчислювальну мережу (ЛОМ) з наявністю підключення до зовнішніх комунікаційних мереж, хоча окремі технічні засоби комплексу ізольовані від мереж. До складу комплексу входять такі технічні засоби: робочі станції (РС) обслуговуючого персоналу (адміністратора безпеки, системного адміністратора та адміністратора реєстрації), центральні сервери ЦСК, внутрішнє комунікаційне обладнання ЛОМ, сервери взаємодії, міжмережевий екран (МЕ) та система виявлення втручань (IDS), комунікаційне обладнання для підключення до зовнішніх мереж, ізольована РС генерації ключів користувачів, РС відокремлених адміністраторів реєстрації.

Апаратні засоби криптографічного захисту інформації

Електронний ключ “Кристал-1”

Електронний ключ «Кристал-1» - це апаратний засіб криптографічного захисту інформації, що виконаний у вигляді малогабаритного з’ємного USB-пристрою та використовується в якості носія ключової інформації. Електронний ключ «Кристал-1» виконує наступні функції: автентифікацію користувача при доступі до ключа, генерацію особистих та відкритих ключів для алгоритму кваліфікованого електронного підпису чи печатки, генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора, зберігання особистих ключів у внутрішній пам’яті та захист їх від несанкціонованого доступу (НСД), формування та перевірку електронного підпису (ЕЦП) чи печатки, обчислення геш-функції та шифрування даних. Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливлює доступ до особистих ключів з боку програмно-апаратного середовища.

Апаратний генератор випадкових чисел “Гряда-4”

Генератор випадкових чисел «Гряда-4» призначений для апаратної генерації послідовностей випадкових чисел на основі фізичних датчиків шуму у складі апаратно-програмних засобів та комплексів криптографічного захисту інформації, що реалізовані на основі ЕОМ. АГВЧ «Гряда-4» виконаний у вигляді малогабаритного пристрою, що має кронштейн для розміщення всередині системного блоку ЕОМ та з’єднується з системною платою ЕОМ через USB-інтерфейс. Швидкість генерації випадкових біт – 200 Кбіт/с.

Мережний криптомодуль “Гряда-301”

Мережний криптомодуль «Гряда-301» призначений для апаратної реалізації криптографічних перетворень у складі центральних серверів центру сертифікації ключів (ЦСК). Пристрій виконує наступні функції: автентифікацію центральних серверів ЦСК чи іншої електронної обчислювальної машини (ЕОМ) при доступі до модуля, генерацію особистих та відкритих ключів для алгоритмів ЕЦП, шифрування та протоколу розподілу ключів, генерацію випадкових послідовностей на основі апаратного генератора, зберігання особистих ключів у внутрішній пам’яті та захист їх від НСД, формування та перевірку ЕЦП, обчислення геш-функції, шифрування, розподіл ключових даних на основі асиметричного протоколу, резервне копіювання ключів.

Мережний криптомодуль реалізує наступні криптографічні алгоритми та протоколи: шифрування за ДСТУ ГОСТ 28147:2009; ЕЦП за ДСТУ 4145-2002, RSA, ECDSA; гешування за ГОСТ 34.311-95; протоколи розподілу ключів Діффі-Гелмана в групі точок еліптичної кривої та RSA.

Криптомодуль “Гряда-61”

Криптографічний модуль «Гряда-61» призначений для апаратної реалізації криптографічних перетворень у складі центральних серверів чи робочої станції адміністраторів сертифікації центру сертифікації ключів (ЦСК) і забезпечує використання та захист особистого ключа. Криптомодуль виконує наступні функції: автентифікацію адміністратора при доступі до пристрою, генерацію особистих та відкритих ключів для алгоритму електронного цифрового підпису (ЕЦП) та протоколу розподілу ключів, генерацію ключів для алгоритму шифрування, генерацію випадкових послідовностей, зберігання ключів та даних у внутрішній пам’яті пристрою та захист їх від несанкціонованого доступу (НСД), формування ЕЦП та шифрування даних.

Пристрій реалізує наступні криптографічні алгоритми та протоколи: шифрування за ДСТУ ГОСТ 28147:2009, ЕЦП за ДСТУ 4145-2002, гешування за ГОСТ 34.311-95 та протокол розподілу ключів Діффі-Гелмана в групі точок еліптичної кривої.

Віддалена лабораторія безпеки ReSeLa+

ReSeLa+ - це програмний комплекс на базі хмарних обчислень, створений для студентів та викладачів університетів, які вивчають чи викладають безпеку інформаційних технологій. Він дозволяє створювати та налаштовувати віртуальні машини із різними операційними системами (Windows, Ubuntu, Kali Linux тощо), динамічно запускати їх на віддалених серверах для виконання лабораторних робіт. Дана лабораторія включає систему із серверного хмарного обладнання та 15 комп'ютерів. Фронтендом комплексу виступає веб-інтерфейс, а бекенд базується на використанні технології OpenStack.