Wojskowy Instytut Łączności - Państwowy Instytut Badawczy

https://wil.waw.pl/wil/oferta/badania-i-rozwoj/zaklad-kryptologii/17627,Zaklad-Kryptologii.html
08.08.2024, 09:26

Zakład Kryptologii

Kierownik - dr inż. Robert Wicik
tel. 261 885 550

Dostarczanie wymaganych przez ustawę urządzeń i narzędzi kryptograficznych oraz kompletnych systemów ochrony informacji niejawnych.

Pełny cykl opracowania: począwszy od prac badawczo-rozwojowych, poprzez certyfikację typu i zgodności, po produkcję i wsparcie przy wdrożeniu.

- Kryptografia i kryptoanaliza
  - oryginalne algorytmy i protokoły kryptograficzne, dopuszczone do ochrony informacji o najwyższych klauzulach tajności
  - analizy bezpieczeństwa algorytmów kryptograficznych i systemów ochrony informacji
- Urządzenia kryptograficzne
  - oryginalne konstrukcje urządzeń kryptograficznych, przeznaczonych do ochrony informacji niejawnych
  - sprzętowe moduły szyfrowania z kryptografią narodową i interoperacyjną
  - oryginalne konstrukcje identyfikatorów użytkowników i elektronicznych nośników danych kryptograficznych
  - sprzętowe generatory ciągów losowych
  - sprzętowe moduły generacji i zabezpieczenia kluczy
- Systemy zarządzania danymi kryptograficznymi
  - podsystemy planowania, generacji i dystrybucji danych kryptograficznych, w tym kluczy
  - podsystemy monitorowania i zarządzania urządzeniami kryptograficznymi
  - podsystemy infrastruktury klucza publicznego

Uzyskane w ostatnich latach certyfikaty ochrony kryptograficznej

Nazwa urządzenia lub narzędzia kryptograficznego	*Nr certyfikatu typu*	*Klauzula chronionych informacji*

LAWENDA - system ochrony informacji w sieciach radiowych. Radiowy Moduł Kryptograficzny wraz z identyfikatorem ID-RMK, Dystrybutor Danych Kryptograficznych wraz z identyfikatorem ID-DDK, Polowa Stacja Planowania Generacji i Dystrybucji Danych Kryptograficznych wraz z identyfikatorami ID-u oraz ID-S	21/2020	ZASTRZEŻONE, NATO RESTRICTED, RESTREINT UE / EU RESTRICTED
RUMIANEK -system ochrony informacji w sieciach ISDN. Terminal BRI ISDN typ RUMIANEK-BRI, Interfejs kryptograficzny PRI ISDN typ RUMIANEK-PRI wraz z zestawem stacji planowania, generacji, ładowania i dystrybucji danych kryptograficznych oraz bankami danych kryptograficznych	58/2017	TAJNE, NATO/EU CONFIDENTIAL
Sprzętowy generator ciągów losowych SGCL-1MB	143/2016	ŚCIŚLE TAJNE