26	Temat	**Ochrona informacji istotnych dla bezpieczeństwa i funkcjonowania państwa, w tym o klauzuli „Ściśle Tajne" - Budowy narodowego centrum kryptografii i dekryptażu.**
	Obszar bezpieczeństwa	Nowoczesne technologie i innowacyjne rozwiązania w zakresie wykrywania, zwalczania i neutralizacji zagrożeń
	Cel główny	Ochrona informacji istotnych dla bezpieczeństwa i funkcjonowania państwa, w tym o klauzuli „Ściśle Tajne"
	Cele szczegółowe	Wytworzenie produktów naukowych - narzędzi matematycznych i informatycznych dotyczących algorytmów, protokołów, metod kryptoanalizy, analiz rozwoju, koncepcji. Wytworzenie produktów technologicznych - oprogramowania kryptograficznego i rozwiązań bezpieczeństwa obejmujących implementację produktów naukowych.
	Czas realizacji projektu	do 48 m-cy
	Oczekiwany poziom gotowości technologicznej	*VIII*
	Instytucja zgłaszająca projekt	Agencja Bezpieczeństwa Wewnętrznego
	Opis projektu	Produkty stanowiące rezultat wdrożenia rozwiązań powstałych z zastosowaniem zaawansowanych technik kryptografii i kryptoanalizy stanowią fundament niezbędny do kompleksowej ochrony informacji, w tym informacji klasyfikowanej. **Z punktu widzenia interesów państwa polskiego występuje konieczność posiadania i rozwoju własnego potencjału intelektualnego i technicznego w zakresie kryptografii i kryptoanalizy.** **Zakres:** Podstawowymi celami programu byłoby wytworzenie: 1. Produktów naukowych - narzędzi matematycznych i informatycznych dotyczących algorytmów, protokołów, metod kryptoanalizy, analiz rozwoju, koncepcji, 2. Produktów technologicznych - oprogramowania kryptograficznego i rozwiązań bezpieczeństwa obejmujących implementację produktów naukowych, w tym efektywnych rozwiązań, prototypów i produktów do: – generowania liczb losowych, – generowania kluczy kryptograficznych, – szyfrowania strumieniowego i blokowego, – szyfrowania symetrycznego, asymetrycznego, – uwierzytelniania osób, – kryptograficznego zabezpieczania danych i systemów informacyjnych, – efektywnego wykorzystywania środowisk do przetwarzania rozproszonego,

		– budowy sprzętowych akceleratorów kryptograficznych, – przesyłania informacji wielostrumieniowych, – kryptoanalizy zabezpieczonej przesyłanej i przechowywanej informacji, – budowy rozwiązań technicznych zabezpieczających przed kanałami podprogowymi oraz manipulacjami dostawców systemów, – innych rozwiązań wymagających zastosowania kryptografii a wynikających z zapotrzebowań beneficjentów. **Oczekiwane efekty:** – powstanie skutecznych i efektywnych, w pełni weryfikowalnych i niezależnych od produktów zagranicznych, rozwiązań do kryptograficznej ochrony przechowywanej i przesyłanej informacji, – rozwój rozwiązań własnych do krypto analizy, – powstanie technik uniezależniających bezpieczeństwo systemów informacyjnych od uczciwości dostawców, – wytworzenie rozwiązań informatycznych wspierających ochronę informacji oklauzulowanej do poziomu tajemnicy państwowej.