

УТВЕРЖДАЮ

Генеральный директор
ООО "Фактор-ТС"

А.В. Бирковский

" " 2012 года



УТВЕРЖДАЮ

Генеральный директор
ООО "КРИПТО-ПРО"

Н.Г. Чернова

" " 2012 года



Протокол

**испытаний соответствия реализации IPsec проектам
методических рекомендаций ТК26 и обеспечения
встречной работы**

Москва, 2012

Общество с ограниченной ответственностью "Фактор-ТС" (ООО "Фактор-ТС") и Общество с ограниченной ответственностью "КРИПТО-ПРО" (ООО "КРИПТО-ПРО"), провели совместные испытания СКЗИ "Dionis NX" и СКЗИ "КриптоПро CSP" на соответствие обязательным требованиям проектов методических рекомендаций ТК26 по реализации протоколов IPsec (ESP, IKE, ISAKMP).

Участники испытаний:

- от ООО "Фактор-ТС":
 - Косых Петр Александрович
 - Подобаев Владимир Николаевич
- от ООО "КРИПТО-ПРО":
 - Леонтьев Сергей Ефимович
 - Пичулин Дмитрий Николаевич

1. Провели испытания СКЗИ "Dionis NX" (аппаратный модуль) и СКЗИ "КриптоПро CSP 3.6R3" (ПО установленное в ОС Windows 7) на стенде на территории ООО "Фактор-ТС", на основании проектов документов:
 - "Методические рекомендации по использованию комбинированного алгоритма шифрования вложений IPsec ESP на основе ГОСТ 28147-89", ТК26, РГ "IPsec и IKE", май 2012;
 - "Методические рекомендации по использованию ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при управлении ключами IKE и ISAKMP", ТК26, РГ "IPsec и IKE", май 2012.
2. Во время испытаний проверены все обязательные пункты рекомендаций со следующими результатами:

	Пункт рекомендаций	Содержание проверяемого пункта рекомендаций	Результаты
1	Требования к IKE и ISAKMP		
1.1	11.1	Алгоритм хэш-функции с идентификатором GOST_R_3411_94	Проверено
1.2	11.2	Алгоритма шифрования с идентификатором GOST-B-CFB-IMIT	Проверено
1.3	11.3	Метод аутентификации IKE с идентификатором IKE-GOST-PSK	Проверено
1.4	11.3	Метод аутентификации IKE с идентификатором IKE-GOST-SIGNATURE	Проверено
1.5	11.4	Группа типа VKO GOST R 34.10-2001 с идентификатором	Проверено

	Пункт рекомендаций	Содержание проверяемого пункта рекомендаций	Результаты
		VKO GOST R 34.10-2001 XchB	
1.6	10.1	Режим "Quick Mode" (QM) без использования PFS	Проверено
1.7	10.1	Режим "Quick Mode" (QM) с использованием PFS	Проверено
2	Требования к ESP		
2.1	6.6	Преобразование ESP_GOST-4M-IMIT	Проверено
2.2	6.7	Преобразование ESP_GOST-1K-IMIT	Проверено
2.3	7.1	Параметры ГОСТ 28147-89 с идентификатором id-Gost28147-89-CryptoPro-B-ParamSet	Проверено
3	Общие требования к реализации IPsec (RFC 2407, 2408, 2409, 4303)		
3.1	RFC 2407 4.5 RFC 4303 3.1.1	Транспортный режим (Transport Mode)	Проверено
2.2	RFC 2407 4.5 RFC 4303 3.1.2	Туннельный режим (Tunnel Mode)	Проверено

3. Значения параметров проектов рекомендаций и IPsec, имеющие значения по умолчанию, устанавливались в эти значения;
4. Опциональные параметры проектов рекомендаций и IPsec при испытаниях не использовались (в том числе, не использовался опциональный атрибут Extended (64-bit) Sequence Number – 11, введён RFC 4304 как расширение RFC 2407);

5. Общий вывод участников: СКЗИ "Dionis NX" и СКЗИ "КриптоПро CSP" соответствуют обязательным требованиям проектов методических рекомендаций ТК26 по реализации протоколов IPsec (ESP, IKE, ISAKMP) и обеспечивают возможность встречной работы.


Подписи участников испытаний:

от ООО "Фактор-ТС":

Косых Петр Александрович

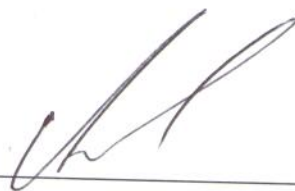
 2 июля 2012 г

Подобаев Владимир Николаевич

 2 июля 2012 г

от ООО "КРИПТО-ПРО":

Леонтьев Сергей Ефимович



Пичулин Дмитрий Николаевич

