УТВЕРЖДАЮ

Генеральный директор
ООО "НТБ"

М.В. Шалаева

"25" 12 2012 года

УТВЕРЖДАЮ

Генеральный директор
ООО "КРИПТО-ПРО"

Н.Г. Чернова

"26" 10 2012 года

Протокол

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

Москва, 2012

Общество с ограниченной ответственностью "Новые технологии безопасности" (ООО «НТБ») и **Общество с ограниченной ответственностью "КРИПТО-ПРО" (ООО "КРИПТО-ПРО")**, провели совместные испытания СКЗИ "StoneGate Firewall/VPN" и СКЗИ "КриптоПро CSP" на соответствие обязательным требованиям проектов методических рекомендаций ТК26 по реализации протоколов IPsec (ESP, IKE, ISAKMP).

Участники испытаний:

- от ООО НТБ:

  Бабенков Сергей Владимирович

  Куликов Андрей Валерьевич

- от ООО "КРИПТО-ПРО":

  Леонтьев Сергей Ефимович

  Пичулин Дмитрий Николаевич

1. Провели испытания СКЗИ "StoneGate Firewall/VPN" версии 5 (аппаратная платформа Stonesoft) и СКЗИ "КриптоПро CSP 3.6R3" (ПО установленное в ОС Windows 2003) на стенде на территории ООО «НТБ», на основании проектов документов:
   - "Методические рекомендации по использованию комбинированного алгоритма шифрования вложений IPsec ESP на основе ГОСТ 28147-89", ТК26, РГ "IPsec и IKE", июль 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", июль 2012.
2. Во время испытаний проверены обязательные и опциональные 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	Обязательный для реализации алгоритм шифрования с идентификатором GOST-B-CFB-IMIT	**Проверено**
1.3	11.2	Опциональные алгоритмы шифрования с идентификаторами: • GOST-A-CFB-IMIT; • GOST-C-CFB-IMIT;	**Проверено**

	Пункт рекомендаций	Содержание проверяемого пункта рекомендаций	Результаты
		• GOST-D-CFB-IMIT.	
1.4	11.3	Метод аутентификации IKE с идентификатором IKE-GOST-PSK	**Проверено**
1.5	11.3	Метод аутентификации IKE с идентификатором IKE-GOST-SIGNATURE	**Проверено**
1.6	11.4	Обязательная для реализации группа типа VKO GOST R 34.10-2001 с идентификатором VKO GOST R 34.10-2001 XchB	**Проверено**
1.7	11.4	Опциональная группа типа VKO GOST R 34.10-2001 с идентификатором VKO GOST R 34.10-2001 XchA	**Проверено**
1.8	10.1	Режим "Quick Mode" (QM) без использования PFS	**Проверено**
1.9	10.1	Режим QM с использованием PFS на основе обязательной для реализации группы с идентификатором VKO GOST R 34.10-2001 XchB	**Проверено**
1.10	10.1	Режим QM с использованием PFS на основе опциональной группы с идентификатором VKO GOST R 34.10-2001 XchA	**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	Обязательные для реализации параметры ГОСТ 28147-89 с идентификатором id-Gost28147-89-CryptoPro-B-ParamSet	**Проверено**

	Пункт рекомендаций	Содержание проверяемого пункта рекомендаций	Результаты
2.4	7.1	Опциональные параметры ГОСТ 28147-89 с идентификаторами: • id-Gost28147-89-CryptoPro-A-ParamSet; • id-Gost28147-89-CryptoPro-C-ParamSet; • id-Gost28147-89-CryptoPro-D-ParamSet.	**Проверено**
2.6	11.1	Опциональный режим совместимости в котором может согласовываться атрибут "Authentication Algorithm" (5) со значением GOST-NULL-INTEGRITY-ALGORITHM (65411)	**Проверено**
3	**Общие требования к реализации IPsec (RFC 2407, 2408, 2409, 3193, 4303)**		
3.2	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. Остальные опциональные параметры проектов рекомендаций и IPsec при испытаниях не использовались;
5. Общий вывод участников: СКЗИ "StoneGate Firewall/VPN" версии 5 и СКЗИ "КриптоПро CSP" версии 3.6R3 соответствуют требованиям проектов методических рекомендаций ТК26 по реализации протоколов IPsec (ESP, IKE, ISAKMP) и обеспечивают возможность встречной работы.

Подписи участников испытаний:

от ООО «НТБ»:

Бабенков Сергей Владимирович

Куликов Андрей Валерьевич

от ООО "КРИПТО-ПРО":

Пичулин Дмитрий Николаевич

Леонтьев Сергей Ефимович