

УТВЕРЖДАЮ

Генеральный директор
ООО "Криптоком"



Д.Б. Кабелев

_____ 2014 г.

УТВЕРЖДАЮ

Генеральный директор
ООО "КРИПТО-ПРО"



Н.Г. Чернова

_____ 2014 г.

ПРОТОКОЛ

испытаний соответствия реализации TLS методическим рекомендациям
ТК26 и обеспечения встречной работы

Москва, 2014

Общество с ограниченной ответственностью "Криптоком" (ООО "Криптоком") и общество с ограниченной ответственностью "КРИПТО-ПРО" (ООО "КРИПТО-ПРО") провели совместные испытания СКЗИ "МагПро КриптоПакет 3.0" и СКЗИ "КриптоПро CSP 4.0" на соответствие требованиям методических рекомендаций ТК26 по использованию российских криптографических алгоритмов в протоколе TLS.

Участники испытаний:

- от ООО "Криптоком":

Устинов Игорь Геннадьевич, заместитель генерального директора;

- от ООО "КРИПТО-ПРО":

Смышляев Станислав Витальевич, начальник отдела защиты информации.

1. Проведены испытания СКЗИ "МагПро КриптоПакет 3.0" (программное обеспечение, установленное на ОС семейства Windows NT) и СКЗИ "КриптоПро CSP4.0" (программное обеспечение, установленное на ОС семейства Windows NT) на основании документов:

- [TLS] Методические рекомендации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS),

- [ALG] Методические рекомендации по криптографическим алгоритмам, сопутствующим применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012;

- [X.509] Техническая спецификация использования алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509.

2. Во время испытаний проверены пункты рекомендаций, включая все обязательные пункты, со следующими результатами:

Реализация полной функциональности серверной и клиентской частей протокола осуществлялась каждым участником испытаний по каждому пункту таблицы.

	Пункт рекомендаций	Содержание проверяемого пункта рекомендаций	Результаты
1	Встречная работа на наборе параметров шифрования TLS_GOSTR341001_WITH_28147_CNT_IMIT		
1.1	5[TLS]	При односторонней аутентификации на сертификате открытого ключа сервера id-GostR3410-2001	Проверено
1.2	5[TLS]	При двусторонней аутентификации на сертификате открытого ключа сервера id-GostR3410-2001и сертификате открытого ключа клиента id-GostR3410-2001	Проверено
2	Встречная работа на наборе параметров шифрования TLS_GOSTR341112_256_WITH_28147_CNT_IMIT		
2.1	5[TLS]	При односторонней аутентификации на сертификате открытого ключа сервера id-GostR3410-2001.	Проверено
2.2	5[TLS] 4.3.1 [X.509]	При односторонней аутентификации на сертификате открытого ключа сервера id-tc26-gost3410-2012-256.	Проверено
2.3	5[TLS] 4.3.1 [X.509]	При односторонней аутентификации на сертификате открытого ключа сервера id-tc26-gost3410-2012-512.	Проверено
2.4	5[TLS]	При двусторонней аутентификации на сертификате открытого ключа сервера id-GostR3410-2001 и сертификате открытого ключа клиента id-GostR3410-2001.	Проверено
2.5	5[TLS] 4.3.1 [X.509]	При двусторонней аутентификации на сертификате открытого ключа сервера id-GostR3410-2001 и сертификате открытого ключа клиента id-tc26-gost3410-2012-256.	Проверено
2.6	5[TLS] 4.3.1 [X.509]	При двусторонней аутентификации на сертификате открытого ключа сервера id-GostR3410-2001 и сертификате открытого ключа клиента id-tc26-gost3410-2012-512.	Проверено
2.7	5[TLS] 4.3.1 [X.509]	При двусторонней аутентификации на сертификате открытого ключа сервера id-tc26-gost3410-2012-256 и сертификате открытого ключа клиента id-GostR3410-2001.	Проверено
2.8	5[TLS] 4.3.1 [X.509]	При двусторонней аутентификации на сертификате открытого ключа сервера id-tc26-gost3410-2012-256 и сертификате открытого ключа клиента id-tc26-gost3410-2012-256.	Проверено

2.9	5[TLS] 4.3.1 [X.509]	При двусторонней аутентификации на сертификате открытого ключа сервера id-tc26-gost3410-2012-256 и сертификате открытого ключа клиента id-tc26-gost3410-2012-512.	Проверено
2.10	5[TLS] 4.3.1 [X.509]	При двусторонней аутентификации на сертификате открытого ключа сервера id-tc26-gost3410-2012-512 и сертификате открытого ключа клиента id-GostR3410-2001.	Проверено
2.11	5[TLS] 4.3.1 [X.509]	При двусторонней аутентификации на сертификате открытого ключа сервера id-tc26-gost3410-2012-512 и сертификате открытого ключа клиента id-tc26-gost3410-2012-256.	Проверено
2.12	5[TLS] 4.3.1 [X.509]	При двусторонней аутентификации на сертификате открытого ключа сервера id-tc26-gost3410-2012-512 и сертификате открытого ключа клиента id-tc26-gost3410-2012-512.	Проверено
3	Корректность использования алгоритмов и их параметров		
3.1	4.2 [TLS]	Использование для передачи premaster_secret алгоритма передачи ключей на основе VKO GOST R 34.10-2001 при сертификате открытого ключа сервера id-GostR3410-2001.	Проверено
3.2	4.2 [TLS] 5.3.1 [ALG]	Использование для передачи premaster_secret алгоритма передачи ключей на основе VKO_GOSTR3410_2012_256 при сертификате сервера открытого ключа id-tc26-gost3410-2012-256 или открытого ключа id-tc26-gost3410-2012-512.	Проверено
3.3	4.3 [TLS]	Использование псевдослучайной функции PRF_GOSTR3411 при использовании набора параметров шифрования TLS_GOSTR341001_WITH_28147_CNT_IMIT.	Проверено
3.4	4.3 [TLS] 5.2.1.1 [ALG]	Использование псевдослучайной функции PRF_TLS_GOSTR3411_2012_256 при использовании набора параметров шифрования TLS_GOSTR341112_256_WITH_28147_CNT_IMIT.	Проверено
3.5	4.4 [TLS]	Использование алгоритма шифрования ГОСТ 28147-89 с набором параметров id-Gost28147-89-CryptoPro-A-ParamSet при использовании набора параметров шифрования TLS_GOSTR341001_WITH_28147_CNT_IMIT.	Проверено
3.6	4.4 [TLS]	Использование алгоритма шифрования ГОСТ	Проверено

		28147-89 с набором параметров id-tc26-gost-28147-param-Z при использовании набора параметров шифрования TLS_GOSTR341112_256_WITH_28147_CNT_IMIT.	
3.7	4.4 [TLS]	Использование функции выработки имитовставки IMIT_GOST28147 с наборами параметров шифрования TLS_GOSTR341001_WITH_28147_CNT_IMIT и TLS_GOSTR341112_256_WITH_28147_CNT_IMIT.	Проверено
3.8	4.5, 5.6 [TLS]	Аутентификация клиента с помощью электронной подписи по ГОСТ Р 34.10-2001: по сертификату открытого ключа id-GostR3410-2001 с использованием алгоритмов (gostr3411, gostr34102001) при сертификате открытого ключа сервера id-tc26-gost3410-2012-256 или id-tc26-gost3410-2012-512.	Проверено
3.9	4.5, 5.6 [TLS]	Аутентификация клиента с помощью электронной подписи по ГОСТ Р 34.10-2012, 256 бит: по сертификату открытого ключа id-tc26-gost3410-2012-256 с использованием алгоритмов (gostr34112012_256, gostr34102012_256) при сертификате открытого ключа сервера id-GostR3410-2001 или id-tc26-gost3410-2012-512.	Проверено
3.10	4.5, 5.6 [TLS]	Аутентификация клиента с помощью электронной подписи по ГОСТ Р 34.10-2012, 512 бит: по сертификату открытого ключа id-tc26-gost3410-2012-512 с использованием алгоритмов (gostr34112012_512, gostr34102012_512) при сертификате открытого ключа сервера id-GostR3410-2001 или id-tc26-gost3410-2012-256.	Проверено

3. Общий вывод участников испытаний: СКЗИ "МагПро КриптоПакет 3.0" и СКЗИ "КриптоПро CSP" соответствуют требованиям рекомендаций ТК26 по реализации протокола TLS и обеспечивают возможность встречной работы.

Подписи участников испытаний:

- от ООО "Криптоком":

 Устинов Игорь Геннадьевич, заместитель генерального директора

- от ООО "КРИПТО-ПРО":

 Смышляев Станислав Витальевич, начальник отдела защиты информации