

УТВЕРЖДАЮ
Заместитель генерального директора
ООО «КРИПТО-ПРО»
С.В. Смышляев
«___» 2024 года

ИЗВЕЩЕНИЕ ОБ ИЗМЕНЕНИЯХ

ООО «КРИПТО-ПРО»	ИЗВЕЩЕНИЕ		ОБОЗНАЧЕНИЕ	
	ЖТЯИ.00101-13.1-2024		ЖТЯИ.00101-13	
ДАТА ВЫПУСКА	СРОК ИЗМЕНЕНИЯ		Лист	Листов
15.02.2024	С момента утверждения извещения об изменениях		1	1
ПРИЧИНА	Обновление по результатам контрольных тематических исследований		КОД 3	
УКАЗАНИЯ О ЗАДЕЛЕ	Не отражается			
УКАЗАНИЯ О ВНЕДРЕНИИ	После проведения контроля			
ПРИМЕНЯЕМОСТЬ	ЖТЯИ.00101-13			
РАЗОСЛАТЬ	ФСБ России, ООО «КРИПТО-ПРО»			
ПРИЛОЖЕНИЕ	Без приложения			
ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ			
1	<p>В документ «ЖТЯИ.00101-13 30 01. КriptoПро CSP. КriptoАРМ. Формуляр» из состава эксплуатационной документации внесены следующие изменения.</p> <p>Раздел «5 Аппаратно-программное средство защиты от НСД» переименован в «5 Модуль доверенной загрузки», и первый абзац этого раздела изложен в редакции:</p> <p>«Изделие «КriptoПро CSP» версия 5.0 R3 KC1 (исполнение 1-КriptoАРМ ГОСТ 3) (ЖТЯИ.00101-13) укомплектовано модулем доверенной загрузки (средством защиты информации от несанкционированного доступа).»</p>			
2	<p>В документ «ЖТЯИ.00101-13 95 01. КriptoПро CSP. КriptoАРМ. Правила пользования» из состава эксплуатационной документации внесены следующие изменения.</p> <p>В раздел «6 Требования по криптографической защите» добавлен пункт 7 с текстом следующего содержания:</p> <p>«7) При использовании СКЗИ для защиты TLS-соединений в роли TLS-сервера под управлением ОС Windows после установки необходимо выполнить следующие действия по настройке используемых криптографических алгоритмов:</p> <p>1. Проверить, что отключено использование устаревших криптонаборов (cipher suite-ов), посмотрев либо в контрольной панели СКЗИ КriptoПро CSP (вкладка «Настройки TLS», секция «Сервер»), либо значение ключа <code>tls_server_disable_legacy_cipher_suites</code> в ветке реестра <code>HKEY_LOCAL_MACHINE\SOFTWARE\[Wow6432Node]\Crypto Pro\Cryptography\CurrentVersion\Parameters\</code> (должно быть равно 1).</p> <p>2. Выполнить перезагрузку компьютера.</p> <p>При использовании СКЗИ для защиты TLS-соединений в роли TLS-сервера под управлением ОС Linux/Unix после установки необходимо выполнить следующие действия по настройке используемых криптографических алгоритмов:</p> <p>1. Отключить использование устаревших криптонаборов, установив значение параметра <code>tls_server_disable_legacy_cipher_suites</code> равным 1 командой</p> <pre>./cpconfig -ini '\config\Parameters' -add long tls_server_disable_legacy_cipher_suites 1</pre> <p>2. Выполнить перезагрузку сервиса <code>cproscsp</code> командой</p> <pre>systemctl restart cproscsp</pre> <p>»</p>			
СОСТАВИЛ	БАШОЯН Р.Р.		Н.КОНТРОЛЬ	
ИЗМЕНЕНИЕ ВНЕС		БАШОЯН Р.Р. 15.02.2024		