

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

ИЗВЕЩЕНИЕ ОБ ИЗМЕНЕНИЯХ

ООО «КРИПТО-ПРО»	ИЗВЕЩЕНИЕ		ОБОЗНАЧЕНИЕ	
	ЖТЯИ.00102-13.1-2024		ЖТЯИ.00102-13	
ДАТА ВЫПУСКА	СРОК ИЗМЕНЕНИЯ		Лист	Листов
15.02.2024	С момента утверждения извещения об изменениях		1	2
ПРИЧИНА	Обновление по результатам контрольных тематических исследований		КОД 3	
УКАЗАНИЯ О ЗАДЕЛЕ	Не отражается			
УКАЗАНИЯ О ВНЕДРЕНИИ	После проведения контроля			
ПРИМЕНЯЕМОСТЬ	ЖТЯИ.00102-13			
РАЗОСЛАТЬ	ФСБ России, ООО «КРИПТО-ПРО»			
ПРИЛОЖЕНИЕ	Без приложения			
ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ			
1	<u>В документ «ЖТЯИ.00102-13 30 01. КристоПро CSP. КристоАРМ. Формуляр» из состава эксплуатационной документации внесены следующие изменения.</u>			
	В разделе «2 Требования к эксплуатации СКЗИ» пункт 2.7 изложен в редакции: «2.7. СКЗИ должно использоваться с модулем доверенной загрузки (МДЗ), сертифицированным ФСБ России.»			
	В разделе «4 Комплектность» в Таблице 4.1 «Комплектация «КристоПро CSP» версия 5.0 R3 KC2 (исполнение 2-КристоАРМ ГОСТ 3)» строка, определяющая наличие в комплектации СКЗИ средства защиты информации от несанкционированного доступа, изложена в редакции:			
	3	Модуль доверенной загрузки (МДЗ), сертифицированный ФСБ России.	см. Примечание, п.ii	
	В разделе «4 Комплектность» примечание ii изложено в редакции: «ii. Необходимо использовать МДЗ, сертифицированный ФСБ России. Поставка осуществляется по согласованию с пользователем.»			
Раздел «5 Аппаратно-программное средство защиты от НСД» переименован в «5 Модуль доверенной загрузки», и первый абзац этого раздела изложен в редакции: «Изделие «КристоПро CSP» версия 5.0 R3 KC2 (исполнение 2-КристоАРМ ГОСТ 3) (ЖТЯИ.00102-13) укомплектовано модулем доверенной загрузки (средством защиты информации от несанкционированного доступа).»				
<u>В документ «ЖТЯИ.00102-13 95 01. КристоПро CSP. КристоАРМ. Правила пользования» из состава эксплуатационной документации внесены следующие изменения.</u>				
Раздел «5 Требования по защите от НСД» переименован в «5 Требования по обеспечению безопасности при эксплуатации СКЗИ»; фрагменты текста вида «аппаратно-программные средства защиты от НСД» и «аппаратно-программного средства защиты от НСД» заменены на «МДЗ».				
СОСТАВИЛ	БАШОЯН Р.Р.		Н.КОНТРОЛЬ	
ИЗМЕНЕНИЕ ВНЕС			БАШОЯН Р.Р. 15.02.2024	

<p>ИЗВЕЩЕНИЕ</p> <p>ЖТЯИ.00102-13.1-2024</p>		<p>ЛИСТ 2</p>
<p>2</p>	<p><u>В документ «ЖТЯИ.00102-13 95 01. КriptoПро CSP. КriptoАРМ. Правила пользования» из состава эксплуатационной документации внесены следующие изменения.</u></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> <ol style="list-style-type: none"> 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). 2. Выполнить перезагрузку компьютера. <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> <ol style="list-style-type: none"> 1. Отключить использование устаревших криптонаборов, установив значение параметра <code>tls_server_disable_legacy_cipher_suites</code> равным 1 командой <div data-bbox="256 1066 1505 1104" style="border: 1px solid black; padding: 2px;"> <pre>./cpconfig -ini '\config\Parameters' -add long tls_server_disable_legacy_cipher_suites 1</pre> </div> <ol style="list-style-type: none"> 2. Выполнить перезагрузку сервиса <code>cproscsp</code> командой <div data-bbox="256 1144 1505 1182" style="border: 1px solid black; padding: 2px;"> <pre>systemctl restart cproscsp</pre> </div>	