ИЗВЕЩЕНИЕ ОБ ИЗМЕНЕНИЯХ

ООО «КРИПТО-ПРО»	ОТД	ИЗВЕЩЕНИЕ		ОБОЗНАЧЕНИЕ		
	ОЛС	ЖТЯИ.00088-01.1-2017		ЖТЯИ.00088-01		
ДАТА ВЫПУСКА		СРОК ИЗМЕНЕНИЯ			Лист	Листов
17.11.2017		С момента утверждения извещения об изменениях ЖТЯИ.00088-01			1	10
ПРИЧИНА		Изменение списка поддерживаемых программно-аппаратных средств			КОД 3	
УКАЗАНИЯ О ЗАДЕЛЕ		Не отражается				
УКАЗАНИЯ О ВНЕДРЕНИИ		После проведения контроля				
ПРИМЕНЯЕМОСТЬ		ЖТЯИ.00088-01				
РАЗОСЛАТЬ		ФСБ России, ООО «ЦСИ», ООО «КРИПТО-ПРО»				
ПРИЛОЖЕНИЕ		Без приложения				

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
1	Изменен список поддерживаемых программно-аппаратных сред. Соответствующие изменения внесены в следующие документы: ЖТЯИ.00088-01 30 01. Формуляр; ЖТЯИ.00088-01 90 01. Описание реализации; ЖТЯИ.00088-01 91 01. Руководство администратора безопасности. Общая часть; ЖТЯИ.00088-01 93 01. Приложение командной строки для подписи и шифрования файлов; ЖТЯИ.00088-01 93 02. Приложение командной строки для работы с сертификатами; ЖТЯИ.00088-01 93 03. Приложение для создания TLS-туннеля; ЖТЯИ.00088-01 95 01. Правила пользования. Старая редакция: «LSB Linux Включает дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x: CentOS 4/5/6/7 (x86, x64, POWER, ARM); ТД ОС АИС ФССП России (GosLinux) (x86, x64); Red OS (x86, x64); Fedora 23/24/25 (x86, x64, ARM); Mandriva Enterprise Server 5, Business Server 1 (x86, x64, ARM); Oracle Linux 4/5/6/7 (x86, x64); OpenSUSE 13.2, Leap 42 (x86, x64, ARM); SUSE Linux Enterprise Server 11SP4/12, Desktop 12 (x86, x64, POWER, ARM); Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER, ARM); Синтез-ОС.РС (x86, x64, POWER, ARM); Ubuntu 10.04/12.04/12.10/13.04/14.04/14.10/15.04/15.10/16.04/16.04.1/16.10 (x86, x64, POWER, ARM); Linux Mint 13/14/15/16/17/18 (x86, x64); Debian 7/8 (x86, x64, POWER, ARM); Astra Linux Special Edition (x86-64).

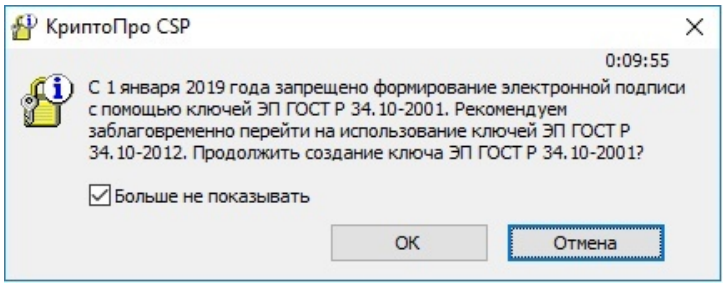
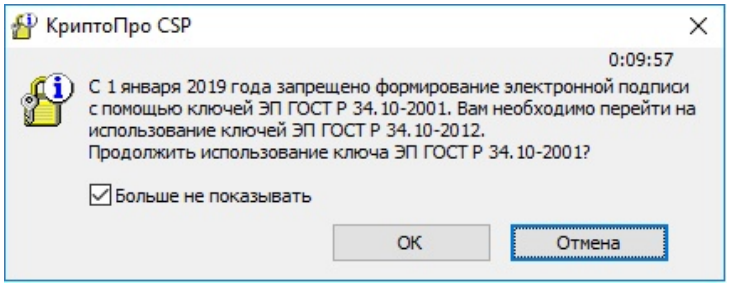
СОСТАВИЛ	МОШНИНА Д.А.			Н.КОНТРОЛЬ		
ИЗМЕНЕНИЕ ВНЕС				МОШНИНА Д.А. 17.11.2017		

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
1	Unix Включает программно-аппаратные среды: ALT Linux 7 (x86, x64, ARM); ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64); РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64); FreeBSD 9/10, pfSense 2.x (x86, x64); AIX 5/6/7 (POWER); Solaris Включает программно-аппаратные среды: Solaris 10 (sparc, x86, x64); Solaris 11 (sparc, x64).» Новая редакция: «LSB Linux Включает дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x: CentOS 4/5/6 (x86, x64); CentOS 7 (x86, x64, POWER, ARM, ARM64); ОСь (OS-RT) (x64); ТД ОС АИС ФССП России (GosLinux) (x86, x64); Red OS (x86, x64); Fedora 25/26/27 (x86, x64, ARM); Oracle Linux 4/5/6 (x86, x64); Oracle Linux 7 (x64); OpenSUSE Leap 42 (x86, x64, ARM, ARM64); SUSE Linux Enterprise Server 11SP4 (x86, x64); SUSE Linux Enterprise Server 12, Desktop 12 (x64, POWER, ARM64); Red Hat Enterprise Linux 4/5/6 (x86, x64); Red Hat Enterprise Linux 7 (x64, POWER, ARM64); Синтез-ОС.РС (x86, x64); Ubuntu 14.04/16.04 (x86, x64, POWER, ARM, ARM64); Ubuntu 17.04/17.10 (x86, x64); Linux Mint 17/18 (x86, x64); Debian 7/8/9 (x86, x64, POWER, ARM, ARM64); Astra Linux Special Edition, Common Edition (x64). Unix Включает программно-аппаратные среды: ALT Linux 6/7 (x86, x64, ARM); Альт Сервер 8, Альт Рабочая станция 8, Альт Рабочая станция К 8 (x86, x64, ARM, ARM64); ROSA Fresh, Enterprise Desktop, Enterprise Linux Server (x86, x64); FreeBSD 9/10/11, pfSense 2.x (x86, x64); AIX 5/6/7 (POWER); РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64); Solaris Включает программно-аппаратные среды: Solaris 10 (sparc, x86, x64); Solaris 11 (sparc, x64).» В документ ЖТЯИ.00088-01 91 03. Руководство администратора безопасности. Linux внесены следующие изменения: Старая редакция: «CentOS 4/5/6/7 (x86, x64, POWER, ARM); ТД ОС АИС ФССП России (GosLinux) (x86, x64);

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
1	Red OS (x86, x64); Fedora 23/24/25 (x86, x64, ARM); Mandriva Enterprise Server 5, Business Server 1 (x86, x64, ARM); Oracle Linux 4/5/6/7 (x86, x64); OpenSUSE 13.2, Leap 42 (x86, x64, ARM); SUSE Linux Enterprise Server 11SP4/12, Desktop 12 (x86, x64, POWER, ARM); Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER, ARM); Синтез-ОС.РС (x86, x64, POWER, ARM); Ubuntu 10.04/12.04/12.10/13.04/14.04/14.10/15.04/15.10/16.04/16.04.1/16.10 (x86, x64, POWER, ARM); Linux Mint 13/14/15/16/17/18 (x86, x64); Debian 7/8 (x86, x64, POWER, ARM); Astra Linux Special Edition (x86-64). ALT Linux 7 (x86, x64, ARM); ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64); РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);» Новая редакция: « CentOS 4/5/6 (x86, x64); CentOS 7 (x86, x64, POWER, ARM, ARM64); ОСь (OS-RT) (x64); ТД ОС АИС ФССП России (GosLinux) (x86, x64); Red OS (x86, x64); Fedora 25/26/27 (x86, x64, ARM); Oracle Linux 4/5/6 (x86, x64); Oracle Linux 7 (x64); OpenSUSE Leap 42 (x86, x64, ARM, ARM64); SUSE Linux Enterprise Server 11SP4 (x86, x64); SUSE Linux Enterprise Server 12, Desktop 12 (x64, POWER, ARM64); Red Hat Enterprise Linux 4/5/6 (x86, x64); Red Hat Enterprise Linux 7 (x64, POWER, ARM64); Синтез-ОС.РС (x86, x64); Ubuntu 14.04/16.04 (x86, x64, POWER, ARM, ARM64); Ubuntu 17.04/17.10 (x86, x64); Linux Mint 17/18 (x86, x64); Debian 7/8/9 (x86, x64, POWER, ARM, ARM64); Astra Linux Special Edition, Common Edition (x64). ALT Linux 6/7 (x86, x64, ARM); Альт Сервер 8, Альт Рабочая станция 8, Альт Рабочая станция К 8 (x86, x64, ARM, ARM64); ROSA Fresh, Enterprise Desktop, Enterprise Linux Server (x86, x64); РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);» В документ ЖТЯИ.00088-01 91 04. Руководство администратора безопасности. FreeBSD внесены следующие изменения: Старая редакция: «СКЗИ «КриптоПро CSP» v 4.0 под управлением ОС FreeBSD используется в программно-аппаратных средах ОС FreeBSD 9/10, pfSense 2.x (x86, x64).»

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
1	Новая редакция: «СКЗИ «КриптоПро CSP» v 4.0 под управлением ОС FreeBSD используется в программно-аппаратных средах ОС FreeBSD 9/10/11, pfSense 2.x (x86, x64).» В документ ЖТЯИ.00088-01 91 05. Руководство администратора безопасности. Solaris внесены следующие изменения: Старая редакция: «СКЗИ «КриптоПро CSP» под управлением ОС типа Solaris используется в следующих программно-аппаратных средах: ОС Solaris 10/11 (sparc, ia32, x64).» Новая редакция: «СКЗИ «КриптоПро CSP» под управлением ОС типа Solaris используется в следующих программно-аппаратных средах: Solaris 10 (sparc, x86, x64); Solaris 11 (sparc, x64).» В документ ЖТЯИ.00088-01 94 01. АРМ выработки внешней гаммы внесены следующие изменения: Старая редакция: «Выработка внешней гаммы и запись ее на отчуждаемые носители производится на автономном АРМ, функционирующем в программно-аппаратной среде Windows 7/2008R2/8/2012/8.1/2012R2/10/2016 (ia32, x64).» Новая редакция: «Выработка внешней гаммы и запись ее на отчуждаемые носители производится на автономном АРМ, функционирующем в следующих программно-аппаратных средах: Windows 7/8/8.1/10/Server 2003/2008 (x86, x64); Windows Server 2008 R2/2012/2012 R2/2016 (x64).» В список поддерживаемых ОС добавлена Windows XP версия POSReady в связи с продолжением поддержки производителем данной версии ОС до апреля 2019 года. В документы ЖТЯИ.00087-01 30 01, ЖТЯИ.00087-01 90 01, ЖТЯИ.00087-01 91 01, ЖТЯИ.00087-01 ЖТЯИ.00087-01 91 02, ЖТЯИ.00087-01 92 01, ЖТЯИ.00087-01 93 01, ЖТЯИ.00087-01 93 02, ЖТЯИ.00087-01 93 03, ЖТЯИ.00087-01 94 01. ЖТЯИ.00087-01 95 01 в списки поддерживаемых программно аппаратных сред добавлена строка: «Windows XP* (x86);». С примечанием * Версия POSReady.
2	В программном коде добавлен параметр force_silent, в документ ЖТЯИ.00088-01 95 01. Правила пользования добавлено его описание. П. 4.2.5. Взаимодействие с пользователем при работе с ключевыми носителями При работе с ключевыми носителями СКЗИ может использовать какой-либо пользовательский интерфейс (UI). Это может происходить, например, при необходимости выбрать носитель или ввести PIN. Чтобы отключить пользовательский интерфейс (например, для автоматизации), в некоторых приложениях существует опция -silent. Также возможно запретить СКЗИ отображать пользовательский интерфейс глобально для всех приложений на данном ПК. Для этого в настройках СКЗИ нужно задать параметр

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
2	force_silent равным единице (см. ниже), force_silent равный нулю вернёт поведение по умолчанию. Если же вызовы функций требуют отображения пользовательского интерфейса, будет возвращена ошибка NTE_SILENT_CONTEXT. Изменение параметра force_silent: Для операционных систем группы Windows необходимо изменить значение ключа реестра HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Crypto Pro\Cryptography\CurrentVersion\Parameters\force_silent (для 64-битных операционных систем), HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\Parameters\force_silent (для 32-битных операционных систем). Настройка СКЗИ для остальных ОС осуществляется с помощью утилиты cpconfig: ./cpconfig -ini '\config\parameters' -add long force_silent 1
3	ЖТЯИ.00088-01 91 03. Руководство администратора безопасности. Linux. ЖТЯИ.00088-01 91 04. Руководство администратора безопасности. FreeBSD ЖТЯИ.00088-01 91 05. Руководство администратора безопасности. Solaris ЖТЯИ.00088-01 91 05. Руководство администратора безопасности. AIX Из списка библиотек, которые должны быть под контролем целостности, исключены следующие библиотеки, не входящие в состав СКЗИ: libpkivalidator.so.4.0.5, libcplib.so.4.0.5, libcpasn1.so.4.0.5, libocsp.so.4.0.5, libenroll.so.4.0.5, libtsp.so.4.0.5, libtspcli.so.4.0.5.
4	ЖТЯИ.00088-01 95 01. Правила пользования В приложении 2 скорректирован комментарий к функции CryptSignHash. Старая редакция: «Разрешено использование только с ключевыми контейнерами, полученными ранее с помощью вызова CertGetCertificateContextProperty из сертификата, проверенного с помощью функции CertVerifyCertificateChainPolicy» Новая редакция: «Разрешено использование только с ключевыми контейнерами, полученными ранее с помощью вызова CryptAcquireCertificatePrivateKey либо с помощью вызова CertGetCertificateContextProperty из сертификата, проверенного с помощью функции CertVerifyCertificateChainPolicy»
5	ЖТЯИ.00088-01 30 01. Формуляр. Из п.п. 5 и 6 убрана подпись главного инженера ООО «КРИПТО-ПРО».
6	ЖТЯИ.00088-01 91 01. Руководство администратора безопасности. Общая часть Добавлено описание предупреждающих окон, появляющихся при использовании ключей алгоритма ГОСТ Р 34.10-2001. «В связи с переходом на использование алгоритма ГОСТ Р 34.10-2012 и соответствующем запрете использования алгоритма ГОСТ Р 34.10-2001 [27], при попытке генерации ключа алгоритма ГОСТ Р 34.10-2001 после 01 июня 2017 года будет выдано следующее предупреждение:

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
6	 Рисунок 6.1 – Предупреждение о генерации ключа для ОС семейства Windows Примечание: на других операционных системах окно внешне может выглядеть по-другому, но текстовая составляющая аналогична приведенной на рисунке. При выборе «Больше не показывать» предупреждения о генерации ключа и создании подписи будут отложены до 01 января 2019 года. При повторном выборе «Больше не показывать» предупреждения более появляться не будут. При попытке создания подписи с использованием ключа алгоритма ГОСТ Р 34.10-2001 после 01 июня 2017 года будет выдано следующее предупреждение.  Рисунок 6.2 – Предупреждение о создании подписи для ОС семейства Windows Примечание: на других операционных системах окно внешне может выглядеть по-другому, но текстовая составляющая аналогична приведенной на рисунке. При выборе «Больше не показывать» предупреждение о создании подписи будет отложено до 01 января 2019 года. При повторном выборе «Больше не показывать» предупреждение более появляться не будет. Создание подписи с использованием ключа алгоритма ГОСТ Р 34.10-2001 с 01 января 2019 года запрещено.» В список литературы добавлено: 27. Порядок перехода к использованию национального стандарта ГОСТ Р 34.10-2012 в средствах электронной подписи для информации, не содержащей сведений, составляющих государственную тайну, в случаях, подлежащих регулированию со стороны ФСБ России в соответствии с действующей нормативной правовой базой [Электронный ресурс]. Режим доступа: https://www.tc26.ru/info/new-national-standards/
7	Уточнена работа с расширениями в ClientHello.
8	Добавлена поддержка АМДЗ «Аккорд» ТУ 4012-054-11443195-2013 и 4012-006-11443195-2005 ТУ, АПМДЗ-У М-526Е1 (КРИПТОН-ЗАМОК/Е) и АПМДЗ «МАКСИМ-М1». В программный код и документацию внесены соответствующие изменения. ЖТЯИ.00087-01 30 01 Формуляр Старая редакция: Таблица 3.3 – Возможные варианты использования различных ДСЧ для выработки случайной последовательности.

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ

ДСЧ/ОС	Windows IA32	Windows x64	Linux	FreeBSD	Solaris	AIX
Физический ДСЧ в составе ПАК защиты от НСД «Соболь» RU.40308570.501410.001 ПС (версии кода расширения BIOS 1.0.99, 1.0.180)	+	+	+	+	-	-
Физический ДСЧ в составе АПМДЗ-У М-526Б (КРИПТОН-ЗАМОК/У) КБДЖ.468243.067 ТУ	+	+	+	-	-	-
Внешняя гамма	+	+	+	+	+	+

Новая редакция:

Таблица 3.2 – Способы формирования закрытых ключей.

ДСЧ/ОС	Windows IA32	Windows x64	Linux	FreeBSD	Solaris	AIX
Физический ДСЧ в составе ПАК защиты от НСД «Соболь» RU.40308570.501410.001 ПС (версии кода расширения BIOS 1.0.99, 1.0.180)	+	+	+	+	-	-
Физический ДСЧ в составе СЗИ НСД «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013, 4012-006-11443195-2005 ТУ	+	+	+	-	-	-
Физический ДСЧ в составе АПМДЗ-У М-526Б (КРИПТОН-ЗАМОК/У) КБДЖ.468243.067 ТУ, М-526Е1 (КРИПТОН-ЗАМОК/Е) КБДЖ.468243.090 ТУ	+	+	-	-	-	-
Физический ДСЧ в составе АПМДЗ «МАКСИМ-М1»	+	+	+	-	-	-
Внешняя гамма	+	+	+	+	+	+

Аналогичные изменения произведены в Таблице 3.2.

8

После таблицы 3.3 добавлено примечание:

«Примечание: Списки версий программно-аппаратных сред, в которых функционируют перечисленные средства защиты от несанкционированного доступа, приведены в документации на соответствующее средства защиты от несанкционированного доступа.»

п. 4 Примечание. Старая редакция: «

1. Для защиты от несанкционированного доступа могут использоваться следующие средства:

- ПАК защиты от НСД «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180);
- Аппаратно-программный модуль доверенной загрузки универсальный М-526Б (КРИПТОН-ЗАМОК/У) КБДЖ.468243.067 ТУ.»

Новая редакция: «

2. Для защиты от несанкционированного доступа могут использоваться следующие средства:

- ПАК защиты от НСД «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180);
- Аппаратно-программный модуль доверенной загрузки универсальный М-526Б (КРИПТОН-ЗАМОК/У) КБДЖ.468243.067 ТУ, М-526Е1 (КРИПТОН-ЗАМОК/Е) КБДЖ.468243.090 ТУ;
- СЗИ НСД «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013, 4012-006-11443195-2005 ТУ;
- АПМДЗ «МАКСИМ-М1».»

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
8	ЖТЯИ.00088-01 91 01. Руководство администратора безопасности. Общая часть Старая редакция: «В качестве программно-аппаратных средств защиты от НСД в СКЗИ могут использоваться Программно-аппаратный комплекс «КРИПТОН-ЗАМОК» и электронный замок «Соболь». Идентификационные данные указанных средств приведены в документе «ЖТЯИ.00088-01 30 01. КриптоПро CSP. Формуляр», п.3.10.» Новая редакция: «В качестве программно-аппаратных средств защиты от НСД в СКЗИ могут использоваться Программно-аппаратный комплекс «КРИПТОН-ЗАМОК», электронный замок «Соболь», АМДЗ «Аккорд» и и АПМДЗ «МАКСИМ-М1». Идентификационные данные указанных средств приведены в документе «ЖТЯИ.00088-01 30 01. КриптоПро CSP. Формуляр», п.3.10.» В документе ЖТЯИ.00088-01 91 02. Руководство администратора безопасности. Windows актуализирован список доступных ДСЧ. Старая редакция: «5.4.4 «Интерфейсные модули ДСЧ Обеспечивают реализацию доступа к следующим типам ДСЧ: – sable.dll ДСЧ электронного замка «Соболь» Новая редакция: «5.4.4 «Интерфейсные модули ДСЧ Обеспечивают реализацию доступа к следующим типам ДСЧ: – sable.dll ДСЧ электронного замка «Соболь» – accord.dll ДСЧ АМДЗ «Аккорд» – apmdz.dll ДСЧ АМДЗ «КРИПТОН-ЗАМОК» – maxim.dll ДСЧ АПМДЗ «МАКСИМ-М1» ЖТЯИ.00088-01 92 01. Инструкция по использованию. Windows Старая редакция: «В исполнении по уровню защиты КС1 предустановлен Биологический ДСЧ. В исполнениях по уровням защиты КС2 и КС3 Биологический ДСЧ или аппаратный ДСЧ «Соболь»/ АПМДЗ-У М-526Б (КРИПТОН ЗАМОК/У) можно добавить в процессе установки криптопровайдера.» Новая редакция: «В исполнении по уровню защиты КС1 предустановлен Биологический ДСЧ. В исполнениях по уровням защиты КС2 и КС3 аппаратный ДСЧ «Соболь» / АПМДЗ-У М-526Б (КРИПТОН ЗАМОК/У), АПМДЗ-Е М-526Е1 (КРИПТОН ЗАМОК/Е) / АМДЗ «МАКСИМ-М1» можно добавить в процессе установки криптопровайдера.».

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
9	Уточнена работа с расширениями в ClientHello.
10	Добавлена поддержка ключевого носителя Rosan, в программный код внесены соответствующие изменения. В Формуляре ЖТЯИ.00088-01 30 01 в Таблицу 3.1 добавлено: <table><tr><th>Носитель/ОС</th><th>Windows IA32</th><th>Windows x64</th><th>Linux</th><th>FreeBSD</th><th>Solaris</th><th>AIX</th></tr><tr><td>Rosan</td><td>+</td><td>+</td><td>+</td><td>+</td><td>+</td><td>-</td></tr></table> В п.3.2 ЖТЯИ.00088-01 90 01, п.6.5 ЖТЯИ.00088-01 91 01, п. 1.3 ЖТЯИ.00088-01 91 02, п. 1.2 ЖТЯИ.00088-01 91 03, п. 1.2 ЖТЯИ.00088-01 91 04, п. 1.2 ЖЯТИ.00088-01 91 05, п. 4.2.1 ЖТЯИ.00088-01 95 01 добавлен носитель Rosan.
11	В Примечании к п. 3.2 ЖТЯИ.00088-01 30 01 операционная система Microsoft Windows Server 2016 внесена в список ОС, для которых необходима серверная лицензия.
12	Microsoft Office Word 2016 добавлен в список программного обеспечения Microsoft, совместно с которым программное обеспечение СКЗИ позволяет использовать российские криптографические алгоритмы и сертификаты открытых ключей стандарта X.509. В п. 6 ЖТЯИ.00088-01 90 01, п. 12 ЖТЯИ.00088-01 91 01, п. 10.3 ЖТЯИ.00088-01 91 02, п. 2 ЖТЯИ.00088-01 95 01 внесены соответствующие изменения.
13	В Формуляр ЖТЯИ.00088-01 30 01 в п. 3.2 добавлено примечание 2 следующего содержания: «2. Необходимо использовать дистрибутивы указанных операционных систем, полученные у разработчика операционной системы, и их штатные репозитории с пакетами. Использование прочих сборок ОС не допускается.» Примечание 2 в старой редакции идет под номером 3 в новой редакции.
14	Перефразирован п. 12 документа ЖТЯИ.00088-01 95 01. Старая редакция: «Разработка программного обеспечения на основе СКЗИ «КриптоПро CSP» с учетом п.1.5 Формуляра ЖТЯИ.00088-01 30 01 может производиться без создания новых СКЗИ в случае использования вызовов из перечня Приложения 2. В случае использования прочих вызовов необходимо производить разработку отдельного СКЗИ в соответствии с действующей нормативной базой (в частности, с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. №313 и Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)).» Новая редакция: «Разработка программного обеспечения на основе СКЗИ «КриптоПро CSP» с учетом п.1.5 Формуляра ЖТЯИ.00088-01 30 01 может производиться без создания новых СКЗИ в случае использования вызовов интерфейсов CryptoAPI СКЗИ из перечня Приложения 2. Данные

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
14	вызовы могут использоваться как напрямую, так и опосредованно через промежуточные интерфейсы. В случае использования (напрямую или опосредованно) в программном обеспечении прочих вызовов интерфейсов CryptoAPI СКЗИ необходимо производить разработку отдельного СКЗИ в соответствии с действующей нормативной базой (в частности, с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. №313 и Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)).»
15	Более не требуется перезагрузка после изменения настроек аудита. В документ ЖТЯИ.00088-01 91 02 внесены соответствующие изменения. В Приложение В добавлено: «Для включения аудита использования КриптоПро TLS на Windows в реестр System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\ добавляется параметр: Значение имени: EventLogging Тип данных: REG_DWORD Параметру присваиваются следующие значения: 0x0000 не записывать в журнал 0x0001 журнал сообщений об ошибках 0x0002 журнал предупреждений 0x0004 журнал информационных событий 0x0008 журнал успешных событий Аудит выполнения процесса cpsspap будет выводиться в журнал приложений Windows. Настройки ведения журнала вступают в силу после пересоздания мандата.»
16	В документе ЖТЯИ.00088-01 30 01 уточнено описание операционных систем, для которых необходима серверная лицензия. Старая редакция: «3. Для следующих ОС необходима серверная лицензия: Microsoft Windows Server 2003; Microsoft Windows Server 2008; Microsoft Windows Server 2008 R2; Microsoft Windows Server 2012; Microsoft Windows Server 2012 R2; Microsoft Windows Server 2016; Все ОС с архитектурой, отличной от x86/x64 (POWER, Sparc); Red Hat Enterprise Linux Server; Ubuntu Server;Solaris; FreeBSD; AIX.» Новая редакция: «3. Для серверного применения СКЗИ (массовое обслуживание) необходима серверная лицензия. Серверными считаются: - ОС семейства Windows Server (2003/2008/2008R2/2012/2012R2/2016); - ОС семейства Linux Server (Red Hat Enterprise Linux Server, SuSE Linux Server, Ubuntu Server, Mandriva Enterprise Server 5, Business Server 1, ROSA Enterprise Linux Server); - Серверные и сетевые ОС (AIX, FreeBSD, Solaris); - Все платформы с серверной процессорной архитектурой (PowerPC, Sparc).»