ИЗВЕЩЕНИЕ ОБ ИЗМЕНЕНИЯХ

<table>
<tr><td rowspan="2">ООО<br>«КРИПТО-ПРО»</td><td>ОТД</td><td colspan="3">ИЗВЕЩЕНИЕ</td><td colspan="3">ОБОЗНАЧЕНИЕ</td></tr>
<tr><td>ОЛС</td><td colspan="3">ЖТЯИ.00087-01.1-2017</td><td colspan="3">ЖТЯИ.00087-01</td></tr>
<tr><td colspan="2">ДАТА ВЫПУСКА</td><td colspan="2">СРОК ИЗМЕНЕНИЯ</td><td rowspan="2"></td><td rowspan="2"></td><td>Лист</td><td>Листов</td></tr>
<tr><td colspan="2">17.11.2017</td><td colspan="2">С момента утверждения извещения об изменениях ЖТЯИ.00087-01</td><td>1</td><td>13</td></tr>
<tr><td colspan="2">ПРИЧИНА</td><td colspan="4">Изменение списка поддерживаемых программно-аппаратных средств и правки документации</td><td colspan="2">КОД<br>3</td></tr>
<tr><td colspan="2">УКАЗАНИЯ О ЗАДЕЛЕ</td><td colspan="6">Не отражается</td></tr>
<tr><td colspan="2">УКАЗАНИЯ О ВНЕДРЕНИИ</td><td colspan="6">После проведения контроля</td></tr>
<tr><td colspan="2">ПРИМЕНЯЕМОСТЬ</td><td colspan="6">ЖТЯИ.00087-01</td></tr>
<tr><td colspan="2">РАЗОСЛАТЬ</td><td colspan="6">ФСБ России, ООО «ЦСИ», ООО «КРИПТО-ПРО»</td></tr>
<tr><td colspan="2">ПРИЛОЖЕНИЕ</td><td colspan="6">Без приложения</td></tr>
<tr><td>ИЗМ:</td><td colspan="7">СОДЕРЖАНИЕ ИЗМЕНЕНИЯ</td></tr>
<tr><td>1</td><td colspan="7">Изменен список поддерживаемых программно-аппаратных сред. Соответствующие изменения внесены в следующие документы:<br>ЖТЯИ.00087-01 30 01. Формуляр;<br>ЖТЯИ.00087-01 90 01. Описание реализации;<br>ЖТЯИ.00087-01 91 01. Руководство администратора безопасности. Общая часть;<br>ЖТЯИ.00087-01 93 01. Приложение командной строки для подписи и шифрования файлов;<br>ЖТЯИ.00087-01 93 02. Приложение командной строки для работы с сертификатами;<br>ЖТЯИ.00087-01 93 03. Приложение для создания TLS-туннеля;<br>ЖТЯИ.00087-01 95 01. Правила пользования.<br>Старая редакция: «LSB Linux<br>Включает дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x:<br>CentOS 4/5/6/7 (x86, x64, POWER, ARM);<br>ТД ОС АИС ФССП России (GosLinux) (x86, x64);<br>Red OS (x86, x64);<br>Fedora 23/24/25 (x86, x64, ARM);<br>Mandriva Enterprise Server 5, Business Server 1 (x86, x64, ARM);<br>Oracle Linux 4/5/6/7 (x86, x64);<br>OpenSUSE 13.2, Leap 42 (x86, x64, ARM);<br>SUSE Linux Enterprise Server 11SP4/12, Desktop 12 (x86, x64, POWER, ARM);<br>Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER, ARM);<br>Синтез-ОС.РС (x86, x64, POWER, ARM);<br>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);<br>Linux Mint 13/14/15/16/17/18 (x86, x64);<br>Debian 7/8 (x86, x64, POWER, ARM, MIPS);<br>Astra Linux Special Edition (x86-64).</td></tr>
<tr><td>СОСТАВИЛ</td><td>МОШНИНА Д.А.</td><td></td><td></td><td>Н.КОНТРОЛЬ</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="4">ИЗМЕНЕНИЕ ВНЕС</td><td colspan="4">МОШНИНА Д.А. 17.11.2017</td></tr>
</table>

| ИЗМ: | СОДЕРЖАНИЕ ИЗМЕНЕНИЯ |
|---|---|
| 1 | Unix<br>Включает программно-аппаратные среды:<br>ALT Linux 7 (x86, x64, ARM);<br>ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64);<br>РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);<br>FreeBSD 9/10, pfSense 2.x (x86, x64);<br>AIX 5/6/7 (POWER);<br>Mac OS X 10.7/10.8/10.9/10.10/10.11/10.12 (x64).<br>Solaris<br>Включает программно-аппаратные среды:<br>Solaris 10 (sparc, x86, x64);<br>Solaris 11 (sparc, x64).<br>iOS<br>Включает программно-аппаратные среды:<br>▪ Apple iOS 6.0/6.0.1/6.0.2/6.1/6.1.2/6.1.3/6.1.4/6.1.5/6.1.6/7.0/7.0.1/7.0.2/7.0.3/7.0.4/7.0.5/7.0.6/7.1/7.1.1/7.1.2/8.0/8.0.1/8.0.2/8.1/8.1.1/8.1.2/8.1.3/8.2/8.3/8.4/8.4.1/9/9.0.1/9.0.2/9.1/9.2/9.2.1/9.3/9.3.1/9.3.2/9.3.3/9.3.4/9.3.5/10 (ARM, arm64, arm7s).»<br>Виртуальные среды<br>Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x64);<br>VMWare WorkStation 11/12 (x86-64);<br>VMWare Player 7/12 (x86, x64);<br>VMWare Sphere ESXi 5.5/6.0 (x64);<br>Virtual Box 3.2/4.0/4.1/4.2/4.3/5.0/5.1 (x86, x64);<br>RHEV 3.4/3.5/3.6/4.0 (x64).»<br>Новая редакция:<br>«LSB Linux<br>Включает дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x:<br>CentOS 4/5/6 (x86, x64);<br>CentOS 7 (x86, x64, POWER, ARM, ARM64);<br>ОСь (OS-RT) (x64);<br>ТД ОС АИС ФССП России (GosLinux) (x86, x64);<br>Red OS (x86, x64);<br>Fedora 25/26/27 (x86, x64, ARM);<br>Oracle Linux 4/5/6 (x86, x64);<br>Oracle Linux 7 (x64);<br>OpenSUSE Leap 42 (x86, x64, ARM, ARM64);<br>SUSE Linux Enterprise Server 11SP4 (x86, x64);<br>SUSE Linux Enterprise Server 12, Desktop 12 (x64, POWER, ARM64);<br>Red Hat Enterprise Linux 4/5/6 (x86, x64);<br>Red Hat Enterprise Linux 7 (x64, POWER, ARM64);<br>Синтез-ОС.РС (x86, x64);<br>Ubuntu 14.04/16.04 (x86, x64, POWER, ARM, ARM64);<br>Ubuntu 17.04/17.10 (x86, x64);<br>Linux Mint 17/18 (x86, x64);<br>Debian 7/8/9 (x86, x64, POWER, ARM, ARM64, MIPS);<br>Astra Linux Special Edition, Common Edition (x64).<br>Unix<br>Включает программно-аппаратные среды:<br>ALT Linux 6/7 (x86, x64, ARM);<br>Альт Сервер 8, Альт Рабочая станция 8, Альт Рабочая станция К 8 (x86, x64, ARM, ARM64);<br>ROSA Fresh, Enterprise Desktop, Enterprise Linux Server (x86, x64);<br>РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64); |

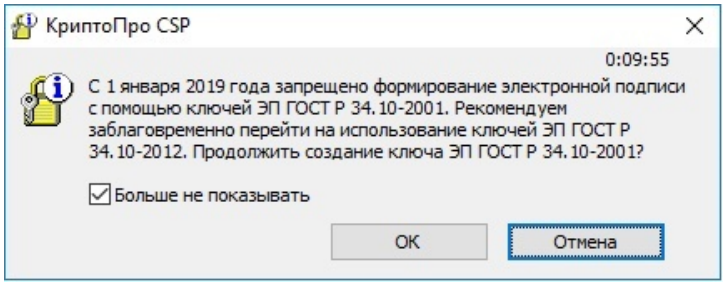
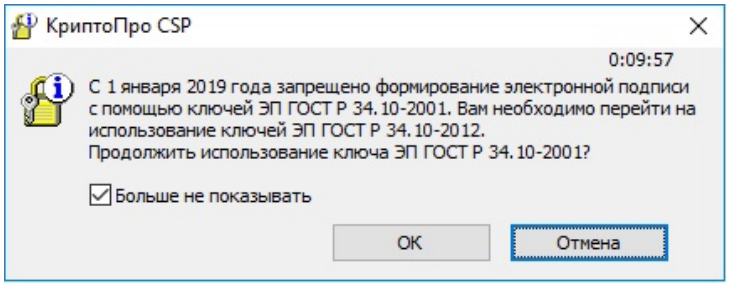
| ИЗМ: | СОДЕРЖАНИЕ ИЗМЕНЕНИЯ |
|---|---|
| 1 | FreeBSD 9/10/11, pfSense 2.x (x86, x64);<br>AIX 5/6/7 (POWER);<br>Mac OS X 10.9/10.10/10.11/10.12 (x64).<br>Solaris<br>Включает программно-аппаратные среды:<br>Solaris 10 (sparc, x86, x64);<br>Solaris 11 (sparc, x64).<br>iOS<br>Включает программно-аппаратные среды:<br>Apple iOS 8.0/8.0.1/8.0.2/8.1/8.1.1/8.1.2/8.1.3/8.2/8.3/8.4/8.4.1/9/9.0.1/9.0.2/9.1/9.2/9.2.1/9.3/9.3.1/9.3.2/9.3.3/9.3.4/9.3.5/10/11 (ARMv7, ARM64).<br>Виртуальные среды<br>Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x64);<br>Microsoft Hyper-V 8/8.1/10 (x64);<br>Citrix XenServer 7.1/7.2 (x64);<br>VMWare WorkStation 11/12 (x86-64);<br>VMWare Player 7/12 (x86, x64);<br>VMWare Sphere ESXi 5.5/6.0 (x64);<br>Virtual Box 3.2/4.0/4.1/4.2/4.3/5.0/5.1 (x86, x64);<br>RHEV 3.4/3.5/3.6/4.0 (x64).»<br>В документ ЖТЯИ.00087-01 91 03. Руководство администратора безопасности. Linux внесены следующие изменения:<br>Старая редакция:<br>«CentOS 4/5/6/7 (x86, x64, POWER, ARM);<br>ТД ОС АИС ФССП России (GosLinux) (x86, x64);<br>Red OS (x86, x64);<br>Fedora 23/24/25 (x86, x64, ARM);<br>Mandriva Enterprise Server 5, Business Server 1 (x86, x64, ARM);<br>Oracle Linux 4/5/6/7 (x86, x64);<br>OpenSUSE 13.2, Leap 42 (x86, x64, ARM);<br>SUSE Linux Enterprise Server 11SP4/12, Desktop 12 (x86, x64, POWER, ARM);<br>Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER, ARM);<br>Синтез-ОС.РС (x86, x64, POWER, ARM);<br>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);<br>Linux Mint 13/14/15/16/17/18 (x86, x64);<br>Debian 7/8 (x86, x64, POWER, ARM);<br>Astra Linux Special Edition (x86-64).<br>ALT Linux 7 (x86, x64, ARM);<br>ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64);<br>РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);»<br>Новая редакция:<br>«CentOS 4/5/6 (x86, x64);<br>CentOS 7 (x86, x64, POWER, ARM, ARM64);<br>ОСь (OS-RT) (x64);<br>ТД ОС АИС ФССП России (GosLinux) (x86, x64);<br>Red OS (x86, x64);<br>Fedora 25/26/27 (x86, x64, ARM); |

| ИЗМ: | СОДЕРЖАНИЕ ИЗМЕНЕНИЯ |
|---|---|
| 1 | Oracle Linux 4/5/6 (x86, x64);<br>Oracle Linux 7 (x64);<br>OpenSUSE Leap 42 (x86, x64, ARM, ARM64);<br>SUSE Linux Enterprise Server 11SP4 (x86, x64);<br>SUSE Linux Enterprise Server 12, Desktop 12 (x64, POWER, ARM64);<br>Red Hat Enterprise Linux 4/5/6 (x86, x64);<br>Red Hat Enterprise Linux 7 (x64, POWER, ARM64);<br>Синтез-ОС.РС (x86, x64);<br>Ubuntu 14.04/16.04 (x86, x64, POWER, ARM, ARM64);<br>Ubuntu 17.04/17.10 (x86, x64);<br>Linux Mint 17/18 (x86, x64);<br>Debian 7/8/9 (x86, x64, POWER, ARM, ARM64, MIPS);<br>Astra Linux Special Edition, Common Edition (x64).<br>ALT Linux 6/7 (x86, x64, ARM);<br>Альт Сервер 8, Альт Рабочая станция 8, Альт Рабочая станция К 8 (x86, x64, ARM, ARM64);<br>ROSA Fresh, Enterprise Desktop, Enterprise Linux Server (x86, x64);<br>РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);»<br><br>В документ ЖТЯИ.00087-01 91 04. Руководство администратора безопасности. FreeBSD внесены следующие изменения:<br>Старая редакция:<br>«СКЗИ «КриптоПро CSP» v 4.0 под управлением ОС FreeBSD используется в программно-аппаратных средах ОС FreeBSD 9/10, pfSense 2.x (x86, x64).»<br>Новая редакция:<br>«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).»<br>В документ ЖТЯИ.00087-01 91 07. Руководство администратора безопасности. MacOS внесены следующие изменения:<br>Старая редакция:<br>«СКЗИ «КриптоПро CSP» под управлением ОС Mac OS X используется в следующих программно-аппаратных средах: Mac OS X 10.7/10.8/10.9/10.10/10.11/10.12 (x64).»<br>Новая редакция:<br>«СКЗИ «КриптоПро CSP» под управлением ОС Mac OS X используется в следующих программно-аппаратных средах: Mac OS X 10.9/10.10/10.11/10.12 (x64).»<br>В документ ЖТЯИ.00087-01 91 08. Руководство администратора безопасности. iOS внесены следующие изменения:<br>Старая редакция:<br>«СКЗИ «КриптоПро CSP» v 4.0 под управлением iOS используется в программно-аппаратных средах iOS версии 6.0, 6.0.1, 6.0.2, 6.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6, 7.0, 7.0.1, 7.0.2, 7.0.3, 7.0.4, 7.0.5, 7.0.6, 7.1, 7.1.1, 7.1.2, 8.0, 8.0.1, 8.0.2, 8.1, 8.1.1, 8.1.2, 8.1.3, 8.2, 8.3, 8.4, 8.4.1, 9, 9.0.1, 9.0.2, 9.1, 9.2, 9.2.1, 9.3, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.5, 10.» |

| ИЗМ: | СОДЕРЖАНИЕ ИЗМЕНЕНИЯ |
|---|---|
| 1 | Новая редакция:<br>«СКЗИ «КриптоПро CSP» v 4.0 под управлением iOS используется в программно-аппаратных средах iOS версии 8.0, 8.0.1, 8.0.2, 8.1, 8.1.1, 8.1.2, 8.1.3, 8.2, 8.3, 8.4, 8.4.1, 9, 9.0.1, 9.0.2, 9.1, 9.2, 9.2.1, 9.3, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.5, 10, 11»<br>В документ ЖТЯИ.00087-01 91 09. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ в виртуальных средах. Внесены следующие изменения:<br>Старая редакция: «<br>Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x64);<br>VMWare WorkStation 11/12 (x86-64);<br>VMWare Player 7/12 (x86, x64);<br>VMWare Sphere ESXi 5.5/6.0 (x64);<br>Virtual Box 3.2/4.0/4.1/4.2/4.3/5.0/5.1 (x86, x64);<br>RHEV 3.4/3.5/3.6/4.0 (x64, POWER).»<br>Новая редакция: «<br>Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x64);<br>Microsoft Hyper-V 8/8.1/10 (x64);<br>Citrix XenServer 7.1/7.2 (x64);<br>VMWare WorkStation 11/12 (x86-64);<br>VMWare Player 7/12 (x86, x64);<br>VMWare Sphere ESXi 5.5/6.0 (x64);<br>Virtual Box 3.2/4.0/4.1/4.2/4.3/5.0/5.1 (x86, x64);<br>RHEV 3.4/3.5/3.6/4.0 (x64, POWER).»<br><br>В раздел 4.2 документа ЖТЯИ.00087-01 91 09 добавлен абзац:<br>«Для XenServer информация о конфигурации виртуальной машины хранится в специализированной базе мета-данных, дублированной на всех хостах (гипервизоре) XenServer. Администратор, обладающий необходимыми правами, может осуществить экспорт виртуальной машины вместе с метаданными в одном из стандартных форматов – VHD или OVF. Тот же администратор может осуществить резервное копирование метаданных виртуальных машин.»<br><br>В раздел 4.4 документа ЖТЯИ.00087-01 91 09 добавлены уточнения:<br>«Помимо обновлений для гостевой ОС и гипервизора, рекомендуется обновлять инструменты виртуализации, такие как VMware Tools, XenTools, а также утилиты, используемые для управления средой виртуализации.»<br>«Также рекомендуется регулярно знакомится с бюллетенями по безопасности, публикуемые производителем гипервизора, для получения информации о найденных уязвимостях и их потенциальном влиянии на инфраструктуру виртуализации.»<br><br>В раздел 4.9 документа ЖТЯИ.00087-01 91 09 добавлено уточнение:<br>Старая редакция:<br>«Примечание - для оперативной памяти выполнение данного требования автоматически обеспечивается средствами Hyper-V и VMWare.»<br>Новая редакция:<br>«Примечание - для оперативной памяти выполнение данного требования автоматически обеспечивается средствами Hyper-V, VMWare и XenServer.» |

| ИЗМ: | СОДЕРЖАНИЕ ИЗМЕНЕНИЯ |
|---|---|
| 1 | В документ ЖТЯИ.00087-01 91 05. Руководство администратора безопасности. Solaris внесены следующие изменения:<br>Старая редакция:<br>«СКЗИ «КриптоПро CSP» под управлением ОС типа Solaris используется в следующих программно-аппаратных средах:<br>ОС Solaris 10/11 (sparc, ia32, x64).»<br><br>Новая редакция:<br>«СКЗИ «КриптоПро CSP» под управлением ОС типа Solaris используется в следующих программно-аппаратных средах:<br>Solaris 10 (sparc, x86, x64);<br>Solaris 11 (sparc, x64).»<br><br>В документ ЖТЯИ.00087-01 94 01. АРМ выработки внешней гаммы внесены следующие изменения:<br>Старая редакция:<br>«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).»<br><br>Новая редакция:<br>«Выработка внешней гаммы и запись ее на отчуждаемые носители производится на автономном АРМ, функционирующем в следующих программно-аппаратных средах:<br>Windows 7/8/8.1/10/Server 2003/2008 (x86, x64);<br>Windows Server 2008 R2/2012/2012 R2/2016 (x64).»<br><br>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:<br>«Windows XP* (x86);».<br>С примечанием * Версия POSReady. |
| 2 | В документ ЖТЯИ.00087-01 91 07. Руководство администратора безопасности. MacOS внесены следующие изменения:<br>1. Поправлена ошибка в наименовании ключевого носителя, п.1.2:<br>Старая редакция: «- USB-токены Рутокен ЭЦП (Flash, Bluetooth), Рутокен Lite Novacard;»<br>Новая редакция: «- USB-токены Рутокен ЭЦП (Flash, Bluetooth), Рутокен Lite;»<br>2. Убрана поддержка Смарткарты УЭК, п.1.2;<br>3. Исправлена ошибка в имени пакета, п.2:<br>Старая редакция: «ru.cryptopro.csp-3.6.1»<br>Новая редакция: «ru.cryptopro.csp-4.0.0»<br>4. Убрано описание пакетов CPROCAdES, CPROOCSPut, CPROTSPutl, CPROnpcades, не входящих в дистрибутив, п.2 Таблица 1.<br>5. п.4.4 |

| ИЗМ: | СОДЕРЖАНИЕ ИЗМЕНЕНИЯ |
|---|---|
| 2 | Старая редакция: «СКЗИ КриптоПро CSP позволяет собирать отладочную информацию и имеет возможность протоколирования событий. Информация записывается в системный журнал (обычно в /var/log/messages).»<br>Новая редакция: «СКЗИ КриптоПро CSP позволяет собирать отладочную информацию и имеет возможность протоколирования событий. Информация записывается в системный журнал (обычно в /var/log/system.log), так же может быть использована утилита «Консоль», являющаяся удобным инструментом просмотра системных событий в Mac OS.»<br>6. Убран п.6.2.6 с описанием библиотеки libasn1data, не входящей в дистрибутив. |
| 3 | В программном коде добавлен параметр force_silent, в документ ЖТЯИ.00087-01 95 01. Правила пользования добавлено его описание.<br>П. 4.2.5. Взаимодействие с пользователем при работе с ключевыми носителями<br>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 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.<br>Изменение параметра force_silent:<br>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).<br>Настройка СКЗИ для остальных ОС осуществляется с помощью утилиты cpconfig:<br>./cpconfig -ini '\config\parameters' -add long force_silent 1 |
| 4 | ЖТЯИ.00087-01 91 03. Руководство администратора безопасности. Linux.<br>ЖТЯИ.00087-01 91 04. Руководство администратора безопасности. FreeBSD<br>ЖТЯИ.00087-01 91 05. Руководство администратора безопасности. Solaris<br>ЖТЯИ.00087-01 91 05. Руководство администратора безопасности. AIX<br>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.<br>ЖТЯИ.00087-01 91 07. Руководство администратора безопасности. MacOS<br>Из списка библиотек, которые должны быть под контролем целостности, исключены следующие библиотеки, не входящие в состав СКЗИ: libcades.1.dylib, ocsputil, libocspcli.4.dylib, tsputil, libpkivalidator.4.dylib, libcplib.4.dylib, libcpasn1.4.dylib, libocsp.4.dylib, libtsp.4.dylib, libtspcli.4.dylib, nmcades, libcppcades.1.dylib, libnpcades.1.dylib, libxmlsec1.1.dylib, libxmlsec1-mscrypto.1.dylib |
| 5 | ЖТЯИ.00087-01 95 01. Правила пользования<br>В приложении 2 скорректирован комментарий к функции CryptSignHash.<br>Старая редакция: «Разрешено использование только с ключевыми контейнерами, полученными ранее с помощью вызова CertGetCertificateContextProperty из сертификата, проверенного с помощью функции CertVerifyCertificateChainPolicy»<br>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» |
| 6 | ЖТЯИ.00087-01 30 01. Формуляр.<br>Из п.п. 5 и 6 убрана подпись главного инженера ООО «КРИПТО-ПРО». |
| 7 | ЖТЯИ.00087-01 91 01. Руководство администратора безопасности. Общая часть<br>Добавлено описание предупреждающих окон, появляющихся при использовании ключей алгоритма ГОСТ Р 34.10-2001. |

| ИЗМ: | СОДЕРЖАНИЕ ИЗМЕНЕНИЯ |
|---|---|
| 7 | «В связи с переходом на использование алгоритма ГОСТ Р 34.10-2012 и соответствующем запрете использования алгоритма ГОСТ Р 34.10-2001 [30], при попытке генерации ключа алгоритма ГОСТ Р 34.10-2001 после 01 июня 2017 года будет выдано следующее предупреждение:<br>  <br><br>Рисунок 6.1 – Предупреждение о генерации ключа для ОС семейства Windows<br>Примечание: на других операционных системах окно внешне может выглядеть по-другому, но текстовая составляющая аналогична приведенной на рисунке.<br>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.<br>При попытке создания подписи с использованием ключа алгоритма ГОСТ Р 34.10-2001 после 01 июня 2017 года будет выдано следующее предупреждение.<br>  <br><br>Рисунок 6.2 – Предупреждение о создании подписи для ОС семейства Windows<br>Примечание: на других операционных системах окно внешне может выглядеть по-другому, но текстовая составляющая аналогична приведенной на рисунке.<br>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.<br>Создание подписи с использованием ключа алгоритма ГОСТ Р 34.10-2001 с 01 января 2019 года запрещено.» |

| ИЗМ: | СОДЕРЖАНИЕ ИЗМЕНЕНИЯ |
|---|---|
| 7 | В список литературы добавлено:<br>30. 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/ |
| 8 | Уточнена работа с расширениями в ClientHello. |
| 9 | Добавлена поддержка АМДЗ «Аккорд» ТУ 4012-054-11443195-2013 и 4012-006-11443195-2005 ТУ, АПМДЗ-У М-526Е1 (КРИПТОН-ЗАМОК/Е) КБДЖ.468243.090 ТУ и АПМДЗ «МАКСИМ-М1». В программный код и документацию внесены соответствующие изменения.<br>ЖТЯИ.00087-01 30 01 Формуляр<br>Старая редакция:<br>Таблица 3.3 – Возможные варианты использования различных ДСЧ для выработки случайной последовательности. |

| ДСЧ/ОС | Windows IA32 | Windows x64 | Linux | FreeBSD | Solaris | AIX | Mac OS X | Apple iOS |
|---|---|---|---|---|---|---|---|---|
| Биологический ДСЧ | + | + | + | + | + | + | + | + |
| 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:

| ДСЧ/ОС | Windows IA32 | Windows x64 | Linux | FreeBSD | Solaris | AIX | Mac OS X | Apple iOS |
|---|---|---|---|---|---|---|---|---|
| Биологический ДСЧ | + | + | + | + | + | + | + | + |
| 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.

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.»

| ИЗМ: | СОДЕРЖАНИЕ ИЗМЕНЕНИЯ |
|---|---|
| 9 | п. 4 Примечание. Старая редакция: «<br>1. Для защиты от несанкционированного доступа могут использоваться следующие средства:<br>– ПАК защиты от НСД «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180);<br>– Аппаратно-программный модуль доверенной загрузки универсальный М-526Б (КРИПТОН-ЗАМОК/У) КБДЖ.468243.067 ТУ.»<br>Новая редакция: «<br>1. Для защиты от несанкционированного доступа могут использоваться следующие средства:<br>– ПАК защиты от НСД «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180);<br>– Аппаратно-программный модуль доверенной загрузки универсальный М-526Б (КРИПТОН-ЗАМОК/У) КБДЖ.468243.067 ТУ, М-526Е1 (КРИПТОН-ЗАМОК/Е) КБДЖ.468243.090 ТУ;<br>– СЗИ НСД «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013, 4012-006-11443195-2005 ТУ;<br>– АПМДЗ «МАКСИМ-М1».»<br><br>ЖТЯИ.00087-01 91 01. Руководство администратора безопасности. Общая часть<br>Старая редакция:<br>«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.00087-01 30 01. КриптоПро CSP. Формуляр», п.3.10.»<br>Новая редакция:<br>«В качестве программно-аппаратных средств защиты от НСД в СКЗИ могут использоваться Программно-аппаратный комплекс «КРИПТОН-ЗАМОК», электронный замок «Соболь», АМДЗ «Аккорд» и АПМДЗ «МАКСИМ-М1». Идентификационные данные указанных средств приведены в документе «ЖТЯИ.00087-01 30 01. КриптоПро CSP. Формуляр», п.3.10.»<br>В документе ЖТЯИ.00087-01 91 02. Руководство администратора безопасности. Windows актуализирован список доступных ДСЧ.<br>Старая редакция: «5.4.5 «Интерфейсные модули ДСЧ<br>Обеспечивают реализацию доступа к следующим типам ДСЧ:<br>– bio.dll БиоДСЧ<br>– sable.dll ДСЧ электронного замка «Соболь» |

| ИЗМ: | СОДЕРЖАНИЕ ИЗМЕНЕНИЯ |
|---|---|
| 9 | Новая редакция: «5.4.5 «Интерфейсные модули ДСЧ<br>Обеспечивают реализацию доступа к следующим типам ДСЧ:<br>– bio.dll БиоДСЧ<br>– sable.dll ДСЧ электронного замка «Соболь»<br>– accord.dll ДСЧ АМДЗ «Аккорд»<br>– apmdz.dll ДСЧ АМДЗ «КРИПТОН-ЗАМОК»<br>– maxim.dll ДСЧ АПМДЗ «МАКСИМ-М1»<br><br>ЖТЯИ.00087-01 92 01. Инструкция по использованию. Windows<br>Старая редакция:<br>«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.»<br><br>Новая редакция:<br>«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.»<br><br>ЖТЯИ.00087-01 95 01 Правила пользования актуализирован список доступных средств защиты от НСД.<br>Старая редакция:<br>«В качестве программно-аппаратных средств защиты от НСД в СКЗИ может использоваться сертифицированный электронный замок «Соболь».»<br>Новая редакция:<br>«В качестве программно-аппаратных средств защиты от НСД в СКЗИ может использоваться сертифицированный электронный замок «Соболь», программно-аппаратный комплекс «КРИПТОН-ЗАМОК», АМДЗ «Аккорд» и АПМДЗ «МАКСИМ-М1».» |
| 10 | Добавлена поддержка ключевого носителя Rosan, в программный код внесены соответствующие изменения. В формуляр ЖТЯИ.00087-01 30 01 в Таблицу 3.1 добавлено: |

| Носитель/ОС | Windows IA32 | Windows x64 | Linux | FreeBSD | Solaris | AIX | Mac OS X | Apple iOS |
|---|---|---|---|---|---|---|---|---|
| Rosan | + | + | + | + | + | - | + | - |

| ИЗМ: | СОДЕРЖАНИЕ ИЗМЕНЕНИЯ |
|---|---|
| 10 | В п.4.2 ЖТЯИ.00087-01 90 01, п.6.5 ЖТЯИ.00087-01 91 01, п. 1.3 ЖТЯИ.00087-01 91 02, п. 1.2 ЖТЯИ.00087-01 91 03, п. 1.2 ЖТЯИ.00087-01 91 04, п. 1.2 ЖЯТИ.00087-01 91 05, п. 1.2 ЖТЯИ.00087-01 91 07, п. 4.2.1 ЖТЯИ.00087-01 95 01 добавлен носитель Rosan. |
| 11 | В Примечании к п. 3.2 ЖТЯИ.00087-01 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.<br>В п. 7 ЖТЯИ.00087-01 90 01, п. 12 ЖТЯИ.00087-01 91 01, п. 10.3 ЖТЯИ.00087-01 91 02, п. 2 ЖТЯИ.00087-01 95 01 внесены соответствующие изменения. |
| 13 | В Формуляр ЖТЯИ.00087-01 30 01 в п. 3.2 добавлено примечание 2 следующего содержания:<br>«2. Необходимо использовать дистрибутивы указанных операционных систем, полученные у разработчика операционной системы, и их штатные репозитории с пакетами. Использование прочих сборок ОС не допускается.»<br>Примечание 2 в старой редакции идет под номером 3 в новой редакции. |
| 14 | Перефразирован п. 12 документа ЖТЯИ.00087-01 95 01.<br>Старая редакция:<br>«Разработка программного обеспечения на основе СКЗИ «КриптоПро CSP» с учетом п.1.5 Формуляра ЖТЯИ.00087-01 30 01 может производиться без создания новых СКЗИ в случае использования вызовов из перечня Приложения 2.<br>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)).»<br>Новая редакция:<br>«Разработка программного обеспечения на основе СКЗИ «КриптоПро CSP» с учетом п.1.5 Формуляра ЖТЯИ.00087-01 30 01 может производиться без создания новых СКЗИ в случае использования вызовов интерфейсов CryptoAPI СКЗИ из перечня Приложения 2. Данные вызовы могут использоваться как напрямую, так и опосредованно через промежуточные интерфейсы.<br>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 |

| ИЗМ: | СОДЕРЖАНИЕ ИЗМЕНЕНИЯ |
|---|---|
| 14 | 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 Приложение В документа ЖТЯИ.00087-01 91 02 внесены соответствующие изменения.<br>Старая редакция:<br>«Для включения аудита использования серверных сертификатов на Windows в реестр<br>System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\<br>добавляется параметр:<br>Значение имени: EventLogging<br>Тип данных: REG_DWORD<br>Параметру присваиваются следующие значения:<br>0x0000 не записывать в журнал<br>0x0001 журнал сообщений об ошибках<br>0x0002 журнал предупреждений<br>0x0004 журнал информационных и успешных событий<br>Аудит выполнения процесса cpsspap будет выводиться в журнал приложений Windows.<br>Ведение журнала вступает в силу только после перезагрузки компьютера.»<br>Новая редакция:<br>«Для включения аудита использования КриптоПро TLS на Windows в реестр<br>System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\<br>добавляется параметр:<br>Значение имени: EventLogging<br>Тип данных: REG_DWORD<br>Параметру присваиваются следующие значения:<br>0x0000 не записывать в журнал<br>0x0001 журнал сообщений об ошибках<br>0x0002 журнал предупреждений<br>0x0004 журнал информационных событий<br>0x0008 журнал успешных событий<br>Аудит выполнения процесса cpsspap будет выводиться в журнал приложений Windows.<br>Настройки ведения журнала вступают в силу после пересоздания мандата.» |
| 16 | В документе ЖТЯИ.00087-01 30 01 уточнено описание операционных систем, для которых необходима серверная лицензия.<br>Старая редакция:<br>«3. Для следующих ОС необходима серверная лицензия:<br>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.»<br>Новая редакция:<br>«3. Для серверного применения СКЗИ (массовое обслуживание) необходима серверная лицензия. Серверными считаются:<br>- ОС семейства Windows Server (2003/2008/2008R2/2012/2012R2/2016);<br>- 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);<br>- Серверные и сетевые ОС (AIX, FreeBSD, Solaris);<br>- Все платформы с серверной процессорной архитектурой (PowerPC, Sparc).» |