УТВЕРЖДАЮ
Генеральный директор
ООО «КРИПТО-ПРО»

_____ Н.Г.Чернова
«__» _____ 2016 года

ИЗВЕЩЕНИЕ ОБ ИЗМЕНЕНИЯХ

ООО «КРИПТО-ПРО»	ОТД	ИЗВЕЩЕНИЕ	ОБОЗНАЧЕНИЕ
	ОЛС	ЖТЯИ.00088-01.1-2016	ЖТЯИ.00088-01

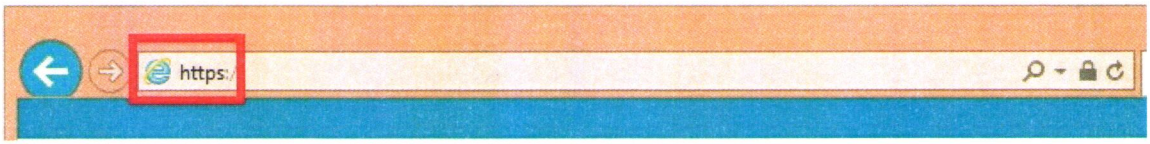
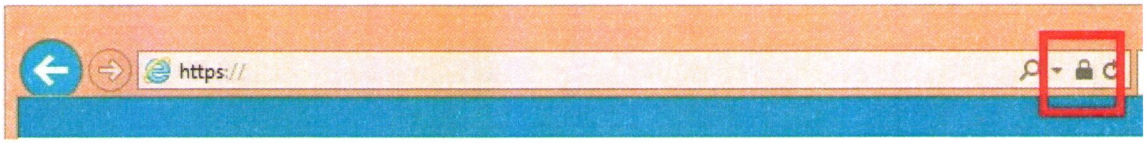
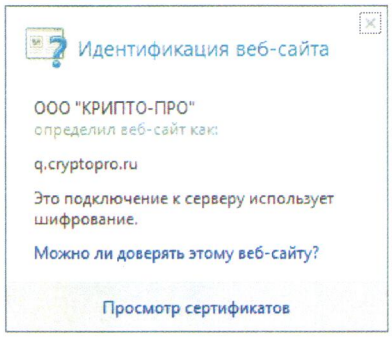
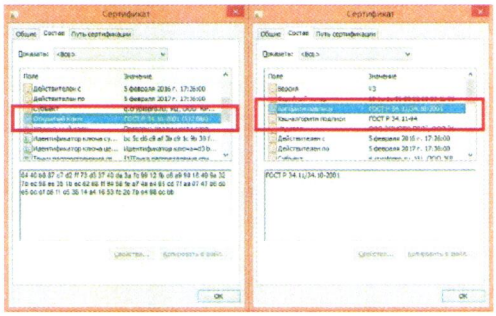
ДАТА ВЫПУСКА	СРОК ИЗМЕНЕНИЯ			Лист	Листов
06.09.2016	С момента утверждения извещения об изменениях ЖТЯИ.00088-01			1	12

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 91 04. Руководство администратора безопасности. FreeBSD; 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: «Windows 7/8/8.1/Server 2003/2008 (x86, x64); Windows Server 2008 R2/2012/2012 R2 (x64). CentOS 4/5/6/7 (x86, x64, POWER, ARM); ТД ОС АИС ФССП России (GosLinux) (x86, x64); Red OS (x86, x64); Fedora 19/20 (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 (x86, x64, POWER, ARM); Linux Mint 13/14/15/16/17 (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); FreeBSD 9, pfSense 2.x (x86, x64); AIX 5/6/7 (POWER);. Solaris 10 (sparc, x86, x64); Solaris 11 (sparc, x64).»

СОСТАВИЛ	МОШНИНА Д.А.			Н.КОНТРОЛЬ		
ИЗМЕНЕНИЕ ВНЕС				МОШНИНА Д.А. 06.09.2016		

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
1	Новая редакция: «Windows 7/8/8.1/10/Server 2003/2008 (x86, x64); Windows Server 2008 R2/2012/2012 R2/2016 (x64). 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). 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 10 (sparc, x86, x64); Solaris 11 (sparc, x64)». Следующие изменения внесены в документ: ЖТЯИ.00088-01 91 04. Руководство администратора безопасности. FreeBSD Старая редакция: «FreeBSD 9, pfSense 2.x (x86, x64)…pkg_add <файл_пакета>…pkg_delete <имя_пакета>» Новая редакция: «FreeBSD 9/10, pfSense 2.x (x86, x64)…pkg_add <файл_пакета> (pkg add <файл_пакета> для FreeBSD 10)…pkg_delete <имя_пакета> (pkg delete <файл_пакета> для FreeBSD 10)». Следующие изменения внесены в документы: ЖТЯИ.00088-01 91 02. Руководство администратора безопасности. Windows и ЖТЯИ.00088-01 94 01. АРМ выработки внешней гаммы. Старая редакция: «Windows 7/8/8.1/Server 2003/2008 (x86, x64); Windows Server 2008 R2/2012/2012 R2 (x64).» Новая редакция: «Windows 7/8/8.1/10/Server 2003/2008 (x86, x64); Windows Server 2008 R2/2012/2012 R2/2016 (x64)». Следующие изменения внесены в документ: ЖТЯИ.00088-01 91 03. Руководство администратора безопасности. Linux. Старая редакция: «CentOS 4/5/6/7 (x86, x64, POWER, ARM); ТД ОС АИС ФССП России (GosLinux) (x86, x64); Red OS (x86, x64); Fedora 19/20 (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 (x86, x64, POWER, ARM); Linux Mint 13/14/15/16/17 (x86, x64); Debian 7/8 (x86, x64, POWER, ARM); Astra Linux Special Edition (x86-64).» Новая редакция: «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).»
2	В документ «ЖТЯИ.00088-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть» добавлено: 7.3 Проверка использования российских алгоритмов в браузере Internet Explorer/Edge. 1. Откройте браузер Internet Explorer/Edge.

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
2	При посещении веб-страницы обратите внимание, используется ли протокол соединения «https».  Рисунок 7.3 – Адресная строка Internet Explorer. 1. Нажмите на значок «замка».  Рисунок 7.4 – Адресная строка Internet Explorer. Должно появится окно следующего вида:  Рисунок 7.5 – Окно идентификации Веб-сайта. 2. Нажмите на Просмотр сертификатов. Откроется SSL сертификат web-сервера. На вкладке «Состав» можно посмотреть информацию об используемых криптографических алгоритмах.  Рисунок 7.6 – Сертификат.

<table>
<tr><th>ИЗМ:</th><th>СОДЕРЖАНИЕ ИЗМЕНЕНИЯ</th></tr>
<tr><td>3</td><td>Добавлена поддержка Microsoft Edge. В следующую документацию внесены соответствующие изменения:
ЖТЯИ.00088-01 90 01. Описание реализации
ЖТЯИ.00088-01 91 01. Руководство администратора безопасности. Общая часть
ЖТЯИ.00088-01 91 02. Руководство администратора безопасности. Windows
Старая редакция: «…Internet Explorer…».
Новая редакция: «…Internet Explorer/ Microsoft Edge …».
В п. 2 документа ЖТЯИ.00088-01 95 01. Правила пользования добавлено: «… Необходимость проведения оценки влияния для прочих программных продуктов (в том числе установленных администратором/пользователем дополнений и расширений программного обеспечения, перечисленного выше) определяется с учетом п.1.5 Формуляра ЖТЯИ.00088-01 30 01…»</td></tr>
<tr><td>4</td><td>Расширен перечень вызовов, использование которых при разработке систем на основе СКЗИ «КриптоПро CSP» версии 4.0 возможно без дополнительных тематических исследований. В «ЖТЯИ.00088-01 95 01. Правила пользования» добавлено:
<table>
<tr><th colspan="3">Дополнительные функции</th></tr>
<tr><td>CryptBinaryToString</td><td>Функция переводит двоичные данные и Base64 и HEX.</td><td></td></tr>
<tr><td>CryptStringToBinary</td><td>Функция переводит строку HEX\Base64 в бинарную строку.</td><td></td></tr>
<tr><td>CertFindAttribute</td><td>Функция производит поиск атрибута сертификата по идентификатору.</td><td></td></tr>
<tr><td>CertGetNameString</td><td>Функция получает имя владельца или издателя сертификата.</td><td></td></tr>
<tr><td>CertNameToStr</td><td>Функция производит раскодирование имени из ASN структуры в DN (RFC1779).</td><td></td></tr>
<tr><td>CertSaveStore</td><td>Функция производит запись хранилища сертификатов (включая списки отозванных и доверенных сертификатов) в виде структуры PKCS#7 или бинарного дампа в память или файл.</td><td></td></tr>
<tr><td>CryptFindCertificateKeyProvInfo</td><td>Функция осуществляет поиск секретного ключа, соответствующего открытому ключу сертификата.</td><td></td></tr>
<tr><td>CryptHashPublicKeyInfo</td><td>Функция осуществляет ASN1 кодирование и хэширование структуры CERT_PUBLIC_KEY_INFO</td><td></td></tr>
<tr><td>CryptMsgCountersign</td><td>Функция вырабатывает добавочную подпись.</td><td></td></tr>
</table>
</td></tr>
</table>

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ

4

CryptMsgCountersignEncoded	Функция вырабатывает добавочную подпись. (кодирует структуру SignerInfo, как определено в PKCS #7).	
CryptMsgVerifyCountersignatureEncoded	Функция проверяет добавочную подпись. (декодирует структуру SignerInfo, как определено в PKCS #7).	
CryptMsgVerifyCountersignatureEncodedEx	Функция проверяет добавочную подпись. (декодирует структуру SignerInfo, как определено в PKCS #7).	

Новая редакция:

CryptCreateHash	Функция CryptCreateHash инициализирует дескриптор нового объекта функции хэширования потока данных.	Разрешено использование только со следующими символьными аргументами: CALG_GR3411, CALG_GR3411_2012_256, CALG_GR3411_2012_512, CALG_GR3411_HMAC, CALG_GR3411_2012_256_HMAC, CALG_GR3411_2012_512_HMAC, CALG_SHAREDKEY_HASH.

6

Изменения документа ЖТЯИ.00088-01 95 01. Правила пользования.

Старая редакция:

«…Разработка программного обеспечения на основе СКЗИ «КриптоПро CSP» может производиться без создания новых СКЗИ в случае использования вызовов из перечня Приложения 2.

Приложение 2. Перечень вызовов, использование которых при разработке систем на основе СКЗИ «КриптоПро CSP» возможно без дополнительных тематических исследований:…»

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 из перечня Приложения 2.

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
6	Приложение 2. Перечень вызовов, использование которых при разработке систем на основе СКЗИ «КриптоПро CSP» с учетом п.1.5 Формуляра ЖТЯИ.00088-01 30 01 возможно без дополнительных тематических исследований:…»
7	В документе ЖТЯИ.00087-01 91 02. Руководство администратора безопасности. Windows скорректирован список системных библиотек, находящихся под контролем целостности. Добавлены библиотеки, перечисленные ниже. Новая редакция:«…**Windows 32-bit** \Windows\system32\inetcomm.dll \Windows\system32\rastls.dll \Windows\system32\wininet.dll \Windows\system32\msi.dll \Windows\system32\crypt32.dll \Windows\system32\schannel.dll \Windows\system32\kerberos.dll \Windows\system32\certenroll.dll \Windows\system32\cryptsp.dll* \Windows\system32\sspicli.dll* *Для ОС Windows Server 2008 под контролем целостности вместо библиотек cryptsp.dll и sspicli.dll находятся библиотеки \Windows\system32\advapi32.dll и \Windows\system32\secur32.dll **Windows 64-bit** \Windows\system32\inetcomm.dll \Windows\SysWOW64\inetcomm.dll \Windows\system32\rastls.dll \Windows\SysWOW64\rastls.dll \Windows\system32\wininet.dll \Windows\SysWOW64\wininet.dll \Windows\system32\msi.dll \Windows\SysWOW64\msi.dll \Windows\system32\crypt32.dll \Windows\SysWOW64\crypt32.dll \Windows\system32\schannel.dll \Windows\SysWOW64\schannel.dll \Windows\system32\kerberos.dll \Windows\SysWOW64\kerberos.dll \Windows\system32\certenroll.dll \Windows\SysWOW64\certenroll.dll \Windows\system32\cryptsp.dll \Windows\SysWOW64\cryptsp.dll* \Windows\system32\sspicli.dll* \Windows\SysWOW64\sspicli.dll* \Windows\SysWOW64\schannel.dll \Windows\system32\kerberos.dll \Windows\SysWOW64\kerberos.dll \Windows\system32\certenroll.dll \Windows\SysWOW64\certenroll.dll \Windows\system32\cryptsp.dll* \Windows\SysWOW64\cryptsp.dll* \Windows\system32\sspicli.dll* \Windows\SysWOW64\sspicli.dll*

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
7	Для ОС Windows Server 2008 под контролем целостности вместо библиотек cryptsp.dll и sspicli.dll находятся библиотеки \Windows\system32\advapi32.dll \Windows\SysWOW64\advapi32.dll \Windows\system32\secur32.dll \Windows\SysWOW64\secur32.dll В случае если целостность данных библиотек нарушена в результате обновления операционной системы, необходимо обратиться к разработчику СКЗИ за разъяснениями о возможности продолжения использования СКЗИ на данной системе.»
8	В документах ЖТЯИ.00088-01 91 01. Руководство администратора безопасности. Общая часть и ЖТЯИ.00088-01 95 01. Правила пользования удалено:«…исключение: дистрибутивы на ОС Windows дополнительно содержат в себе значение подписи в формате Microsoft Authenticode…»
9	В следующие документы внесены изменения порядка контроля действия ключей: ЖТЯИ.00088-01 91 01. Руководство администратора безопасности. Общая часть ЖТЯИ.00088-01 91 02. Руководство администратора безопасности. Windows 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 06. Руководство администратора безопасности. AIX ЖТЯИ.00088-01 91 07. Руководство администратора безопасности. Mac OS Старая редакция: «При формировании закрытого ключа в контейнер записывается дата истечения срока действия этого ключа, по истечении которого в зависимости от настроек групповой политики возможны различные варианты использования этого ключа. Значение «0» групповой политики не накладывает никаких ограничений на использование ключа; Значение «1» групповой политики запрещает формирование ЭП и шифрование в контексте этого ключа (возможно расшифрованные ранее зашифрованных сообщений); Значение «2» групповой политики запрещает любые действия с закрытым ключом.

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
9	Срок действия ключа берется из (в порядке уменьшения приоритета): – Расширения контейнера ключа; – Расширения сертификата ключа; – Даты создания ключа + 1 год 3 месяца. Для операционных систем группы Windows выставить необходимое значение групповой политики можно в Редакторе локальной групповой политики (Выполнить -> gpedit.msc), в разделе «Классические административные шаблоны (ADM)». Для ключей алгоритма ГОСТ Р 34.10-2001 необходимо изменить значение ключа реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Crypto-Pro\CSP\ControlKeyTimeValidity2001. Выставление значения «0» для ключей алгоритма ГОСТ Р 34.10-2001 не допускается. Для ключей алгоритма ГОСТ Р 34.10-2012 как для коротких (256 бит), так и для длинных (512 бит) необходимо изменить значение ключа реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Crypto-Pro\CSP\ ControlKeyTimeValidity2012. Настройка СКЗИ для остальных ОС осуществляется с помощью утилиты cpconfig с помощью команды cpconfig -policy -set ControlKeyTimeValidity2001(2012) -value <значение>. 📖 При работе в режиме усиленного контроля использования ключей (режим обязателен к использованию, отключение может производиться только в целях тестирования) значение групповой политики контроля срока действия пользовательских ключей принимается равным «2». …» Новая редакция: «… При формировании закрытого ключа в контейнер записывается дата истечения срока действия этого ключа, по истечении которого в зависимости от значения параметра ControlKeyTimeValidity возможны различные варианты использования этого ключа. Значение «0» параметра не накладывает никаких ограничений на использование ключа.

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
9	Значение «1» параметра запрещает формирование ЭП и шифрование в контексте этого ключа (возможно расшифрованные ранее зашифрованных сообщений) (значение по умолчанию); Значение «2» параметра запрещает любые действия с закрытым ключом. Срок действия ключа берется из (в порядке уменьшения приоритета): – Расширения контейнера ключа; – Расширения сертификата ключа; – Даты создания ключа + 1 год 3 месяца. Изменение параметра ControlKeyTimeValidity Для операционных систем группы Windows необходимо изменить значение ключа реестра HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Crypto Pro\Cryptography\CurrentVersion\Parameters\ControlKeyTimeValidity (для 64-битных операционных систем), HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\Parameters\ControlKeyTimeValidity (для 32-битных операционных систем). Настройка СКЗИ для остальных ОС осуществляется с помощью утилиты cpconfig с помощью команды ./cpconfig -ini \config\parameters -add long ControlKeyTimeValidity <значение> 📖 При работе в режиме усиленного контроля использования ключей (режим обязателен к использованию, отключение может производиться только в целях тестирования) значение параметра ControlKeyTimeValidity принимается равным «2». …» ЖТЯИ.00088-01 91 08. Руководство администратора безопасности. iOS Добавлено: «… При встраивании СКЗИ КриптоПро CSP в приложения iOS должен быть включён режим усиленного контроля использования ключей. Режим усиленного контроля использования ключей обеспечивает осуществление контроля срока действия долговременных ключей электронной подписи и ключевого обмена, контроля доверенности ключей проверки электронной подписи и контроля корректного использования программного датчика случайных чисел. Для включения этого режима в конфигурационный файл config.ini в раздел [Parameters] необходимо добавить строку: StrengthenedKeyUsageControl = 1

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
9	Для обеспечения корректного функционирования провайдера в части выработки электронной подписи, а также работы с временными ключами (в частности, для работы в рамках TLS-соединения без аутентификации клиента) и генерации случайных данных необходимо произвести выработку долговременных ключей, предварительно проверив, что зарегистрирован хотя бы один датчик случайных чисел. Использование СКЗИ без включения режима усиленного контроля использования ключей разрешается исключительно в тестовых целях. …»
10	Описан механизм работы утилиты cpverify с электронными подписями в документах ЖТЯИ.00088-01 91 02. Руководство администратора безопасности. Windows и ЖТЯИ.00088-01 95 01. Правила пользования. «…- cpverify -file_verify имя_файла [значение_подписи] -timestamp дата Проверка подписи файла с именем «имя_файла». Параметр «значение_подписи» необходимо передавать в виде байтовой строки. Если параметр «значение_подписи» не указан, то значение подписи берется из файла имя_файла.sgn. Параметр «дата» указывает, когда подпись была сформирована, необходимо указывать в формате дд.мм.гггг. Данная команда проверяет подпись с прямой последовательностью полубайт, для проверки подписи с обратной последовательностью байт необходимо использовать команду versign с аналогичным набором параметров. Подпись проверяется на открытом ключе из специального сертификата для подписи кода компании «КРИПТО-ПРО». - cpverify –pe_sign FileName [критерии поиска сертификата] [доп. параметры] Добавление в файл с именем FileName цифровой подписи в формате authenticode полностью на российских алгоритмах с помощью Microsoft CryptoAPI. С помощью данной команды можно подписать только файлы форматов .exe и .dll. Для того чтобы подписать файл, необходимо в хранилище «Личное» текущего пользователя иметь установленный сертификат со ссылкой на закрытый ключ, в назначениях которого присутствует «Подписывание кода». Поиск нужного сертификата осуществляется с помощью следующих критериев: -name SubjectName Имя субъекта сертификата подписи. Это значение может быть подстрокой полного имени субъекта.

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
10	-alg AlgId Алгоритм хэширования для подписи в сертификате. Допустимые значения GR3411, GR3411_2012_256, GR3411_2012_512. -fp FingerPrint Значение sha1 отпечатка сертификата. -append Подпись будет добавлена как второстепенная. Если в файле нет основной подписи или параметр –append не передан, то подпись будет добавлена как основная. Если несколько сертификатов удовлетворяют заданным критериям, то пользователю будет предоставлена возможность вручную выбрать нужный сертификат. - cpverify –pe_verify FileName [доп. параметры] Проверка authenticode подписи файла с именем FileName без использования Microsoft CryptoAPI. -multiple Проверка всех authenticode подписей, найденных в файле. Если параметр не передан, то будет проверена только основная подпись.…»
11	Для блокирования сбора телеметрии на ОС Windows 10/Server 2016 при загрузке операционной системы до старта системных служб удаляются конфигурации службы диагностики (DiagTrack) и записи событий трассировки (AutoLogger-DiagTrack-Listener) при включенном усиленном контроле. Служба диагностики и сборщики данных удаляются из системы и более не могут быть запущены. В документ ЖТЯИ.00088-01 91 02. Руководство администратора безопасности. Windows добавлено: «Для отключения функций телеметрии на ОС Windows 10/Server 2016 необходимо выполнить следующие действия: 1. Проверить наличие и статус сервиса DiagTrack (Панель управления -> Система и безопасность -> Администрирование -> Службы). 2. Если сервис запущен, то остановить его. 3. Удалить запись регистрации сервиса DiagTrack из реестра (Пуск -> выполнить -> regedit, раздел HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services. Здесь необходимо найти и удалить папку DiagTrack). 4. Удалить подготовленные к отправке данные, которые сохраняются в четырех файлах с расширением *.rbs, хранящихся в директории *%ProgramData%\Microsoft\Diagnosis*. Имена файлов для production сборок ОС – event00.rbs, event01.rbs, event10.rbs и event11.rbs. Для insider сборок ОС имена могут отличаться, поэтому необходимо удалить все файлы с расширением *.rbs. При

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
11	возникновении проблем с удалением данных файлов необходимо в свойствах на вкладке «Безопасность» разрешить полный доступ к файлу, а затем удалить. 5. Остановить автоматическую (AutoLogger) ETW сессию *AutoLogger-DiagTrack-Listener*, которую DiagTrack активирует в процессе своей остановки. 6. Удалить файл, в который автоматическая (AutoLogger) ETW сессия *AutoLogger-DiagTrack-Listener* сохраняла собранные данные. Путь к файлу хранится в реестровой записи *AutoLogger-DiagTrack-Listener* в значении *FileName*. Конфигурации автоматических (AutoLogger) ETW сессий находятся в ключе реестра *HKLM\SYSTEM\CurrentControlSet\Control\WMI\AutoLogger*. Конфигурация целевой сессии хранится в данном ключе под записью *AutoLogger-DiagTrack-Listener*. В настоящее время данные сохраняются в файл *%ProgramData%\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-DiagTrack-Listener.etl.* 7. Удалить запись регистрации конфигурации автоматической (AutoLogger) ETW сессии *AutoLogger-DiagTrack-Listener* из реестра Данные действия необходимо выполнять после каждого кумулятивного обновления, поскольку данные обновления являются по сути полной переустановкой ОС и удаленные сервисы восстанавливаются.
12	В документ ЖТЯИ.00088-01 96 01. КриптоПро CSP. Руководство программиста добавлено: «Совместно с дистрибутивом поставляются следующие пакеты, позволяющие интегрировать «КриптоПро CSP» версии 4.0 в приложения, использующие OpenSSL API (такие как Web-сервер ngnix): cprocsp-cpopenssl, cprocsp-cpopenssl-base, cprocsp-cpopenssl-devel, cprocsp-cpopenssl-gost. Подробнее об их установке и настройке можно узнать на портале техподдержки и форуме КриптоПро.»
13	Изменения документа ЖТЯИ.00088-01 30 01. Формуляр. Старая редакция: «Для защиты от несанкционированного доступа могут использоваться следующие средства:…» Новая редакция: «В качестве средства защиты от несанкционированного доступа необходимо использовать одно из следующих средств защиты, при условии наличия действующего сертификата соответствия ФСБ России:…»