ИЗВЕЩЕНИЕ ОБ ИЗМЕНЕНИЯХ

ООО «КРИПТО-ПРО»	ИЗВЕЩЕНИЕ			ОБОЗНАЧЕНИЕ	
	ЖТЯИ.00091-02.1-2018			ЖТЯИ.00091-01	
ДАТА ВЫПУСКА	СРОК ИЗМЕНЕНИЯ			Лист	Листов
10.09.2018	С момента сертификации ЖТЯИ.00091-02			1	15
ПРИЧИНА	Перенос срока запрета формирования электронной подписи по ГОСТ Р 34.10-2001 и другие изменения			КОД 3	
УКАЗАНИЯ О ЗАДЕЛЕ	Не отражается				
УКАЗАНИЯ О ВНЕДРЕНИИ	После проведения контроля				
ПРИМЕНЯЕМОСТЬ	ЖТЯИ.00091-01				
РАЗОСЛАТЬ	ФСБ России, ООО «КРИПТО-ПРО»				
ПРИЛОЖЕНИЕ	Без приложения				

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
1	В связи с продлением возможности использовать ГОСТ Р 34.10-2001 для формирования ЭП на год срок запрета перенесён с 31 декабря 2018 года на 31 декабря 2019 года. Обновлены ограничения в документации, а также отключены соответствующие проверки по датам в программном коде. ЖТЯИ.00091-01 30 01. Формуляр. Старая редакция: « Использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи после 31 декабря 2018 года не допускается. » Новая редакция: « Использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи после 31 декабря 2019 года не допускается. »
2	Изменен список поддерживаемых программно-аппаратных сред. Соответствующие изменения внесены в следующие документы: ЖТЯИ.00091-01 30 01. Формуляр; ЖТЯИ.00091-01 90 01. Описание реализации; ЖТЯИ.00091-01 91 01. Инструкция по использованию.

СОСТАВИЛ	ЛАРИНА Т.М.			Н.КОНТРОЛЬ		
ИЗМЕНЕНИЕ ВНЕС				ЛАРИНА Т.М. 10.09.2018		

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
2	ЖТЯИ.00091-01 30 01. Формуляр, ЖТЯИ.00091-01 90 01. Описание реализации. Старая редакция: «Windows Windows Vista/7/8/8.1 (x86, x64) (только совместно с Java-машиной производства Oracle); Windows Server 2003/2008/2008 R2/2012/2012 R2 (x64) (только совместно с Java-машиной производства Oracle); LSB Linux ОС Linux, удовлетворяющие стандарту Linux Standart Base ISO/IEC 23360 (x86, x64) версии LSB 4.x: CentOS 4/5/6/7 (x86, x64); Fedora 23/24/25 (x86, x64); Mandriva Enterprise Server 5, Business Server 1 (x86, x64); Oracle Linux 5/6/7 (x86, x64); OpenSUSE 12.2/12.3/13.1/13.2 (x86, x64); SUSE Linux Enterprise 10/11/12 (x86, x64, POWER); Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER); 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); Linux Mint 13/14/15/16/17/18 (x86, x64); Debian 7/8 (x86, x64, POWER); Unix ALT Linux 6/7 (x86, x64); ALT Linux 6/7 (ARM) (только совместно с Java-машиной производства Oracle); Ubuntu Phone (ARM) (только совместно с Java-машиной производства Oracle); ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64); РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64); FreeBSD 8/9/10, pfSense 2.x (x86, x64); AIX 5/6/7 (POWER) (только совместно с Java-машиной производства IBM); Mac OS X 10.7/10.8/10.9/10.10/10.11/10.12 (x64); Solaris 10 (sparc, x86, x64) (только совместно с Java-машиной производства Oracle); Solaris 11 (sparc, x64) (только совместно с Java-машиной производства Oracle). » Новая редакция: « Windows Windows Vista/7/8/8.1/10 (x86, x64) (только совместно с Java-машиной производства Oracle); Windows Server 2003/2008/2008 R2/2012/2012 R2/2016 (x64) (только совместно с Java-машиной производства Oracle); LSB Linux ОС Linux, удовлетворяющие стандарту Linux Standart Base ISO/IEC 23360 (x86, x64) версии LSB 4.x:

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
2	CentOS 4/5/6/7 (x86, x64); ТД ОС АИС ФССП России (GosLinux) (x86, x64); Red OS (x86, x64); Fedora 23/24/25/26/27 (x86, x64); Mandriva Enterprise Server 5, Business Server 1 (x86, x64); Oracle Linux 5/6/7 (x86, x64); OpenSUSE 12.2/12.3/13.1/13.2 (x86, x64); SUSE Linux Enterprise 10/11/12 (x86, x64, POWER); Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER); Ubuntu 10.04/12.04/12.10/13.04/14.04/14.10/15.04/15.10/16.04/16.04.1/16.10/17.04/17.10/18.04 (x86, x64, POWER); Linux Mint 13/14/15/16/17/18 (x86, x64); Debian 7/8/9 (x86, x64, POWER); Unix ALT Linux 6/7 (x86, x64); ALT Linux 6/7 (ARM) (только совместно с Java-машиной производства Oracle); Ubuntu Phone (ARM) (только совместно с Java-машиной производства Oracle); ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64); РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64); FreeBSD 8/9/10/11/pfSense 2.x (x86, x64); AIX 5/6/7 (POWER) (только совместно с Java-машиной производства IBM); Mac OS X 10.7/10.8/10.9/10.10/10.11/10.12 (x64); Solaris 10 (sparc, x86, x64) (только совместно с Java-машиной производства Oracle); Solaris 11 (sparc, x64) (только совместно с Java-машиной производства Oracle). » ЖТЯИ.00091-01 91 01. Инструкция по использованию. Старая редакция: « Установка «КриптоПро JCP» версия 2.0 должна осуществляться администратором. На Windows Vista/2008/7/2008R2/8/2012/8.1/2012R2 запуск командного файла следует выполнять как "Run as administrator". » Новая редакция: « Установка «КриптоПро JCP» версия 2.0 должна осуществляться администратором. На Windows Vista/2008/7/2008R2/8/2012/8.1/2012R2/10/2016 запуск командного файла следует выполнять как "Run as administrator". » Старая редакция: « Клиентские ОС: • Windows 2000 Professional; • Windows Vista; • Windows 7/8/8.1; • Red Hat Enterprise Linux X.X Desktop; • Red Hat Enterprise Linux X.X Workstation; (WS)

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
2	• Fedora X; • SUSE Linux Enterprise Desktop XX; • OpenSUSE Linux XX.X; • Debian GNU/Linux X.X; • Mandriva Corporate Desktop X; • Ubuntu X.XX Desktop Edition; • Linux XP Enterprise Desktop 2008; • ALT Linux X.X Desktop; • ALT Linux X.X Lite. Серверные ОС: • Windows 2000 Server; • Windows 2003; • Windows 2008; • Windows 2008R2; • Windows 2012; • Windows 2012R2; • Solaris; • FreeBSD; • AIX; • HP-UX; • любые ОС на архитектуре отличной от ia32/amd64; » Новая редакция: « Клиентские ОС: • Windows 2000 Professional; • Windows Vista; • Windows 7/8/8.1/10; • Red Hat Enterprise Linux X.X Desktop; • Red Hat Enterprise Linux X.X Workstation; (WS) • Fedora X; • SUSE Linux Enterprise Desktop XX; • OpenSUSE Linux XX.X; • Debian GNU/Linux X.X; • Mandriva Corporate Desktop X; • Ubuntu X.XX Desktop Edition; • Linux XP Enterprise Desktop 2008; • ТД ОС АИС ФССП России (GosLinux) (x86, x64); • Red OS (x86, x64); • ALT Linux X.X Desktop; • ALT Linux X.X Lite. Серверные ОС: • Windows 2000 Server; • Windows 2003; • Windows 2008; • Windows 2008R2; • Windows 2012; • Windows 2012R2; • Windows 2016;

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
2	• Solaris; • FreeBSD; • AIX; • HP-UX; • любые ОС на архитектуре отличной от ia32/amd64; »
3	Изменены версии Java-машин, под которыми функционирует СКЗИ. Соответствующие изменения внесены в следующие документы: ЖТЯИ.00091-01 30 01. Формуляр; ЖТЯИ.00091-01 91 01. Инструкция по использованию; ЖТЯИ.00091-01 33 01. Руководство программиста. ЖТЯИ.00091-01 30 01. Формуляр. Старая редакция: « ... функционирует под управлением следующих Java-машин: • Java-машина производства Oracle «Java(TM) 2 Runtime Environment, Standard Edition версии 1.6 и выше на 32-битной и 64-битной платформе. • Java-машины J9VM производства IBM «Java(TM) 2 Runtime Environment, Standard Edition» версии 1.6 и выше на 32-битной и 64-битной платформе. » Новая редакция: « ... функционирует под управлением следующих Java-машин: • Java-машина производства Oracle «Java(TM) 7 Runtime Environment, Standard Edition» версии 1.7 и «Java(TM) 8 Runtime Environment, Standard Edition» версии 1.8 на 32-битной и 64-битной платформе. • Java-машина производства Oracle «Java(TM) 10 Runtime Environment, Standard Edition» версии 10 и «Java(TM) 11 Runtime Environment, Standard Edition» версии 11 на 64-битной платформе. • Java-машины J9VM производства IBM «Java(TM) 7 Runtime Environment, Standard Edition» версии 1.7 и «Java(TM) 8 Runtime Environment, Standard Edition» версии 1.8 на 32-битной и 64-битной платформе. » ЖТЯИ.00091-01 91 01. Инструкция по использованию. Старая редакция: « Криптопровайдер «КриптоПро JCP» версия 2.0 является средством криптографической защиты информации (СКЗИ «КриптоПро JCP» версия 2.0), реализующим российские криптографические алгоритмы и функционирующим под управлением виртуальной машины Java 2 Runtime Environment версии 1.6 и выше. Криптопровайдер «КриптоПро JCP» версия 2.0 должен использоваться с сертифицированными SUN Java-машинами, соответствующим требованиям безопасности SUN. Защищенность криптографических объектов, создаваемых и обрабатываемых криптопровайдером, зависит от степени защищенности и корректности Java-машины, и может быть снижена при использовании виртуальных машин, не имеющих сертификата SUN. Список сертифицированных Java-машин находится на сайте SUN по адресу: http://java.sun.com/j2se/licensees/index.html »

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
3	Новая редакция: « Криптопровайдер «КриптоПро JCP» версия 2.0 является средством криптографической защиты информации (СКЗИ «КриптоПро JCP» версия 2.0), реализующим российские криптографические алгоритмы и функционирующим под управлением виртуальной машины Java 2 Runtime Environment версии 1.7 и 1.8. Криптопровайдер «КриптоПро JCP» версия 2.0 должен использоваться с сертифицированными Oracle Java-машинами, соответствующим требованиям безопасности Oracle. Защищенность криптографических объектов, создаваемых и обрабатываемых криптопровайдером, зависит от степени защищенности и корректности Java-машины, и может быть снижена при использовании виртуальных машин, не имеющих сертификата Oracle. Список сертифицированных Java-машин находится на сайте Oracle по адресу: http://www.oracle.com/technetwork/java/javase/downloads » ЖТЯИ.00091-01 33 01. Руководство программиста. Старая редакция: « Криптопровайдер «КриптоПро JCP» версия 2.0 является средством криптографической защиты информации (СКЗИ «КриптоПро JCP» версия 2.0), реализующим российские криптографические алгоритмы и функционирующим под управлением виртуальной машины Java 2 Runtime Environment версии 1.6 и выше, соответствующей спецификации Sun Java 2 TM Virtual Machine. » Новая редакция: « Криптопровайдер «КриптоПро JCP» версия 2.0 является средством криптографической защиты информации (СКЗИ «КриптоПро JCP» версия 2.0), реализующим российские криптографические алгоритмы и функционирующим под управлением виртуальной машины Java 2 Runtime Environment версии 1.7 и 1.8, соответствующей спецификации Sun Java 2 ™ Virtual Machine. »
4	Добавлена поддержка носителя Rutoken под управлением Mac OS X. Соответствующие изменения внесены в следующие документы: ЖТЯИ.00091-01 30 01. Формуляр; ЖТЯИ.00091-01 90 01. Руководство администратора безопасности. ЖТЯИ.00091-01 30 01. Формуляр. Старая редакция: « 3.9 Хранение закрытых ключей производится на следующих типах носителей:

Носители/ОС	**Windows IA32**	**Windows x64**	**Linux**	**FreeBSD**	**Solaris**	**AIX**	**Mac OS X**
ГМД 3,5'', USB диски	+	+	+	+	+	-	+
eToken, JaCarta	+	+	+	-	-	-	-

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ

Смарткарты Оскар с использованием считывателей, совместимых с OpenCard Framework	+	+	+	-	-	-	+
Rutoken	+	+	+	-	-	-	-
Раздел HDD ПЭВМ	+	+	+	+	+	+	+

»

Новая редакция:

«

Хранение закрытых ключей производится на следующих типах носителей:

Носители/ОС	**Windows**	**Linux**	**FreeBSD**	**Solaris**	**AIX**	**Mac OS X**
ГМД 3,5”, USB диски	+	+	+	+	-	+
eToken, JaCarta	+	+	-	-	-	-
Смарткарты Оскар с использованием считывателей, совместимых с OpenCard Framework	+	+	-	-	-	+
Rutoken	+	+	-	-	-	+
Раздел HDD ПЭВМ	+	+	+	+	+	+

»

ЖТЯИ.00091-01 90 01. Руководство администратора безопасности.

4

В п. 17.2.4. добавился абзац:

«

Rutoken

ru.CryptoPro.JCP.KeyStore.RutokenStore.Install; установщик пакета находится в файле R.jar

»

Также в связи с этим добавился раздел 17.5, описывающий процесс установки и использования модуля поддержки Rutoken.jar.

ЖТЯИ.00091-01 91 01. Инструкция по использованию.

В п. 3.2.3 добавился абзац:

«

Rutoken

Библиотека (модуль) поддержки rutoken.

»

В п. 3.2.4 добавился абзац:

«

Rutoken

ru.CryptoPro.JCP.KeyStore.RutokenStore.Install; установщик пакета находится в файле Rutoken.jar

»

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
5	Изменение названия папки с «Doc» на «javadoc». ЖТЯИ.00091-01 33 01. Руководство программиста. Старая редакция: « Документация CAdES, включающая описание классов и методов, а также примеры работы, находится в папке «Doc» дистрибутива в файле CAdES-javadoc.jar. Полные тексты примеров создания, проверки, усовершенствования, заверения и т. д. находятся в пакете CAdES файла samples-sources.jar. » Новая редакция: « Документация CAdES, включающая описание классов и методов, а также примеры работы, находится в папке «javadoc» дистрибутива в файле CAdES-javadoc.jar. Полные тексты примеров создания, проверки, усовершенствования, заверения и т. д. находятся в пакете CAdES файла samples-sources.jar. »
6	Появилась возможность при создании или усовершенствовании подписи передать CRL для проверки цепочки подписанта. ЖТЯИ.00091-01 33 01. Руководство программиста. п. 9. Старая редакция: «`// Добавляем CAdES-BES подпись №1.`» Новая редакция: «`// Добавляем CAdES-BES подпись №1. Также можно передать CRL для проверки цепочки подписанта вместо использования enableCRLDP`» п. 10 Старая редакция: «`// добавляем подписанта формата XAdES-BES`» Новая редакция: «`// добавляем подписанта формата XadES-BES. Также можно передать CRL для проверки цепочки подписанта вместо использования enableCRLDP`»
7	Отражена поддержка формата подписи XadES-X Long Type 1. ЖТЯИ.00091-01 33 01. Руководство программиста. Раздел 10. Старая редакция: « 10. Использование библиотеки XAdES.jar для создания и проверки подписи формата XAdES-BES и XAdES-T »

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
7	Новая редакция: « 10. Использование библиотеки XAdES.jar для создания и проверки подписи формата XadES-BES, XadES-T и XadES-X Long Type 1 » Старая редакция: « Документация XAdES, включающая описание классов и методов, а также примеры работы, находится в папке Doc дистрибутива в файле XAdES-javadoc.jar. Полные тексты примеров создания и проверки находятся в пакете xades файла samples-sources.jar. XAdES предоставляет XAdES API, в который входят классы XAdESSignature и XAdESSigner. Поддерживается создание подписей формата: 1. XAdES-BES 2. XAdES-T » Новая редакция: « Документация XAdES, включающая описание классов и методов, а также примеры работы, находится в папке javadoc дистрибутива в файле XAdES-javadoc.jar. Полные тексты примеров создания и проверки находятся в пакете xades файла samples-sources.jar. XAdES предоставляет XAdES API, в который входят классы XAdESSignature и XAdESSigner. Поддерживается создание подписей формата: • XAdES-BES • XadES-T • XadES-X Long Type 1 »
8	Добавились новые параметры утилиты keytool: -keystore – можно задать путь хранилища, в котором будет храниться ключ; -storepass – задание пароля на хранилище; -keypass – задание пароля на ключ. ЖТЯИ.00091-01 33 01. Руководство программиста. Раздел 10. Старая редакция: « Таким образом, генерация ключевой пары и запись ее на носитель осуществляется: `keytool -genkeypair -alias myKey -keysize 512 -providername JCP -storetype HDImageStore -keyalg GOST3410EL -sigalg GOST3411withGOST3410EL` » Новая редакция: « Таким образом, генерация ключевой пары и запись ее на носитель осуществляется:

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
8	`keytool -genkeypair -alias myKey -keysize 512 -providername JCP -storetype HDImageStore -keyalg GOST3410EL -sigalg GOST3411withGOST3410EL -keystore c:\.keystore -storepass 123456 -keypass 11111111` »
9	К реализуемым сюитам относится только TLS_CIPHER_2001 и TLS_CIPHER_2012. Убрана поддержка SSL-сюит. ЖТЯИ.00091-01 33 03. Руководство программиста (JTLS). п. 5.1 Старая редакция: « Ниже приводится таблица с кратким описанием реализуемых «КриптоПро JTLS» версия 2.0 криптонаборов:

Имя криптонабора	Идентификатор криптонабора	Алгоритм ключей обмена	Режим шифрования данных по алгоритму ГОСТ Р 28147-89
TLS_CIPHER_2012	0xff85	ГОСТ 34.10-2012	Гаммирование
TLS_CIPHER_2001	0x81	ГОСТ 34.10-2001	Гаммирование
SSL3_CK_GVO_KB2	0x32	ГОСТ 34.10-2001	Гаммирование с обратной связью
SSL3_CK_GVO	0x31	ГОСТ 34.10-2001	Гаммирование с обратной связью

»

Новая редакция:

«

Ниже приводится таблица с кратким описанием реализуемых «КриптоПро JTLS» версия 2.0 криптонаборов:

Имя криптонабора	Идентификатор криптонабора	Алгоритм ключей обмена	Режим шифрования данных по алгоритму ГОСТ Р 28147-89
TLS_CIPHER_2012	0xff85	ГОСТ 34.10-2012	Гаммирование
TLS_CIPHER_2001	0x81	ГОСТ 34.10-2001	Гаммирование

»

п. 5.2.

Старая редакция:

«

- **TLS_CIPHER_2012** - поддерживается обеими сторонами. Если данная сторона является сервером, и в полученном ею списке поддерживаемых клиентом криптонаборов содержится *TLS_CIPHER_2012*, то именно он и выбирается в качестве рабочего. Если данная сторона является клиентом, то криптонабор *TLS_CIPHER_2012* отправляется первым в списке поддерживаемых.
- **TLS_CIPHER_2001** - поддерживается обеими сторонами. Если данная сторона является сервером, и в полученном ею списке поддерживаемых клиентом криптонаборов содержится *TLS_CIPHER_2001*, то именно он и выбирается в качестве рабочего. Если данная сторона является клиентом, то криптонабор *TLS_CIPHER_2001* отправляется первым в списке поддерживаемых.

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
9	• **SSL3_CK_GVO_KB2** - поддерживается обеими сторонами. Если данная сторона является сервером, и в полученном ею списке поддерживаемых клиентом криптонаборов не содержалось *TLS_CIPHER_2001*, то в качестве рабочего выбирается *SSL3_CK_GVO_KB2* (при условии, что она содержится в списке). Если данная сторона является клиентом, то криптонабор *SSL3_CK_GVO_KB2* отправляется второй в списке поддерживаемых. **SSL3_CK_GVO** - поддерживается сервером и опционально клиентом (по умолчанию клиентом не поддерживается). Если данная сторона является сервером, и в полученном ею списке поддерживаемых клиентом криптонаборов не содержалось ни *TLS_CIPHER_2001*, ни *SSL3_CK_GVO_KB2* , то в качестве рабочей выбирается *SSL3_CK_GVO*. Если данная сторона является клиентом, то по умолчанию она данный криптонабор не поддерживает. Следовательно, данный криптонабор не заносится в отправляемый серверу список, а если в ответ на переданный список сервер ответил данным криптонабором, то считается, что обмен не может быть осуществлен. *Однако, для поддержки старых серверов (например, DIGT), реализована возможность опционального подключения криптонабора SSL3_CK_GVO в список, поддерживаемых клиентом криптонаборов. Данное подключение может быть осуществлено при помощи системной настройки* `System.setProperty("javax.net.ssl.supportGVO","true")`. *Такое подключение не рекомендуется к использованию. После того, как криптонабор подключен, он будет занесен в список поддерживаемых клиентом криптонаборов последним.* Таким образом, формируются следующие списки поддерживаемых криптонаборов: **Клиент** / **Сервер** TLS_CIPHER_2012 / TLS_CIPHER_2012 TLS_CIPHER_2001 / TLS_CIPHER_2001 SSL3_CK_GVO_KB2 / SSL3_CK_GVO_KB2 SSL3_CK_GVO (опционально) / SSL3_CK_GVO » Новая редакция: « • **TLS_CIPHER_2012** - поддерживается обеими сторонами. Если данная сторона является сервером, и в полученном ею списке поддерживаемых клиентом криптонаборов содержится *TLS_CIPHER_2012*, то именно он и выбирается в качестве рабочего. Если данная сторона является клиентом, то криптонабор *TLS_CIPHER_2012* отправляется первым в списке поддерживаемых. • **TLS_CIPHER_2001** - поддерживается обеими сторонами. Если данная сторона является сервером, и в полученном ею списке поддерживаемых клиентом криптонаборов содержится *TLS_CIPHER_2001*, то именно он и выбирается в качестве рабочего. Если данная сторона является клиентом, то криптонабор *TLS_CIPHER_2001* отправляется первым в списке поддерживаемых. Таким образом, формируются следующие списки поддерживаемых криптонаборов:

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ

Клиент	**Сервер**
TLS_CIPHER_2012	TLS_CIPHER_2012
TLS_CIPHER_2001	TLS_CIPHER_2001

»

9

п. 5.3.

Старая редакция:

«

Ниже приводится таблица, в которой описывается, какой именно криптонабор будет выбран сервером при условии при осуществлении процесса обмена с различными версиями «КриптоПро JTLS» версия 2.0.

Клиент	**Сервер**	**Выбираемый сервером криптонабор**
JTLS 2.0	JTLS 2.0	TLS_CIPHER_2012, TLS_CIPHER_2001
JTLS 2.0/ CSP 4.0	CSP 4.0/ JTLS 2.0	TLS_CIPHER_2012, TLS_CIPHER_2001
JTLS 2.0/ CSP 3.6	CSP 3.6/ JTLS 2.0	TLS_CIPHER_2001
JTLS 2.0	CSP 2.0	SSL3_CK_GVO_KB2
JTLS 2.0	CSP 3.0	TLS_CIPHER_2001
CSP 2.0	JTLS 2.0	SSL3_CK_GVO
CSP 3.0	JTLS 2.0	TLS_CIPHER_2001

»

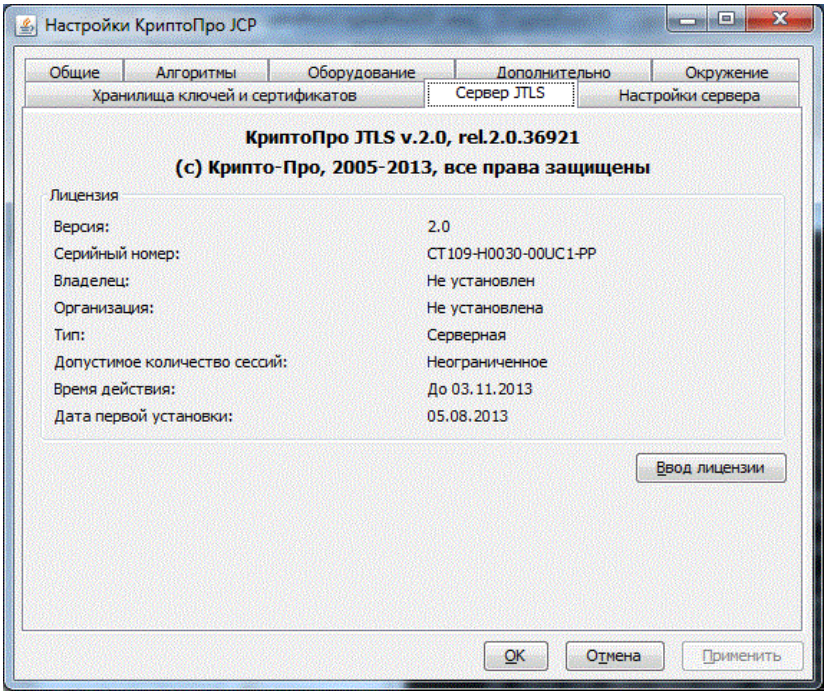
Новая редакция:

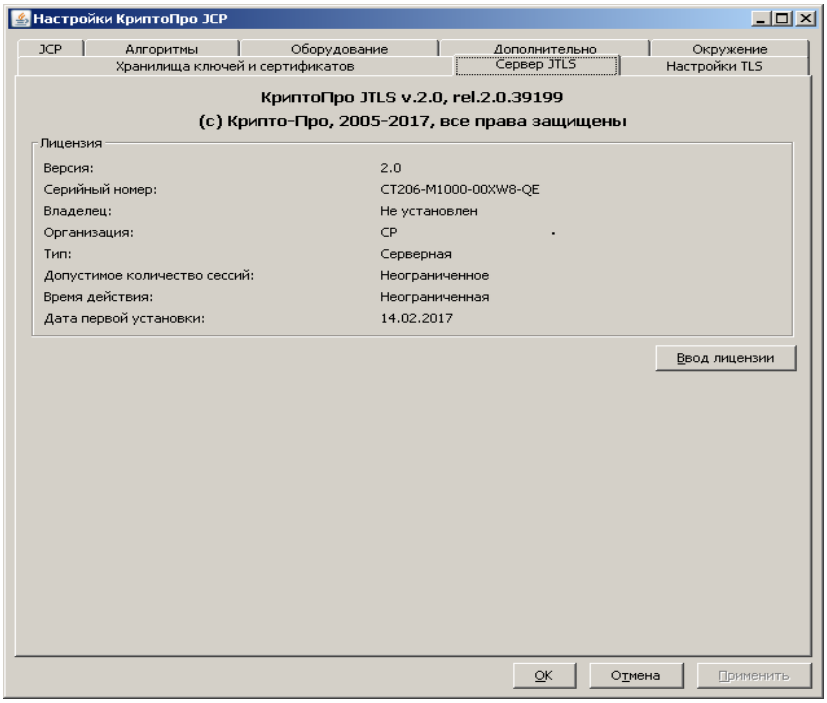
«

Ниже приводится таблица, в которой описывается, какой именно криптонабор будет выбран сервером при условии при осуществлении процесса обмена с различными версиями «КриптоПро JTLS» версия 2.0.

Клиент	**Сервер**	**Выбираемая сервером криптонабор**
JTLS 2.0	JTLS 2.0	TLS_CIPHER_2012, TLS_CIPHER_2001
JTLS 2.0/ CSP 4.0	CSP 4.0/ JTLS 2.0	TLS_CIPHER_2012, TLS_CIPHER_2001

»

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
10	ЖТЯИ.00091-01 91 01. Инструкция по использованию, ЖТЯИ.00091-01 91 02. Инструкция по использованию (JTLS). Добавился новый раздел: «Настройка параметров провайдера с помощью Preferences». Данный раздел «Инструкции по использованию» и «Инструкции по использованию (JTLS)» описывает процесс настройки JCP и Java TLS соответственно путем редактирования параметров провайдера, хранящихся в Preferences. Добавился новый раздел: «6. Использование утилиты ComLine». ЖТЯИ.00091-01 91 01. Инструкция по использованию В разделе 6 приведен порядок работы с утилитой ComLine, позволяющей выполнять следующие операции: • проверка установки и настроек провайдеров • проверка работоспособности провайдеров • работа с ключами и сертификатами использование КриптоПро JTLS.
11	Изменено название вкладки «Общие» на «JCP» панели управления. Изменения были внесены в следующие документы: ЖТЯИ.00091-01 33 03. Руководство программиста (JTLS) (п. 6.1.). ЖТЯИ.00091-01 91 02. Инструкция по использованию (JTLS) (п. 2.1.). Старая редакция: «  **Рисунок 1. Внешний вид панели "Лицензия" (временная лицензия)** Данная панель содержит информацию о серверной лицензии «КриптоПро JTLS» версия 2.0. Работа с данной панелью аналогична работе с закладкой "Общие" (панель "Лицензия"). »

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
11	Новая редакция: «  **Рисунок 1. Внешний вид панели "Лицензия" (временная лицензия)** Данная панель содержит информацию о серверной лицензии «КриптоПро JTLS» версия 2.0. Работа с данной панелью аналогична работе с закладкой "JCP" (панель "Лицензия"). »
12	Добавлена возможность при установке провайдера указать провайдер по умолчанию и создать ярлык для запуска панели управления. Соответствующие изменения были внесены в следующие документы: ЖТЯИ.00091-01 90 01. Руководство администратора безопасности (п. 17.2). ЖТЯИ.00091-01 91 01. Инструкция по использованию (п. 3.2.1). Добавлен абзац: « При установке провайдера можно указать, какой из них будет использоваться по умолчанию. В дальнейшем эту настройку можно изменить в панели JCP на закладке «Алгоритмы». В зависимости от приоритета тот или иной провайдер будет находиться выше в списке провайдеров java.security. » Старая редакция: « После перехода далее в случае установки может быть предложено запустить панель управления «КриптоПро JCP» версия 2.0. » Новая редакция: «

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
12	После перехода далее в случае установки может быть предложено запустить панель управления «КриптоПро JCP» версия 2.0 и создать ярлык для запуска ControlPanel на Рабочем столе. »
13	Добавлены новые параметры, которые можно указать в конфигурационном файле утилиты tls_proxy. В параметрах соединений («Parameters») появилась возможность явно указать название провайдера и протокол соединения. А в параметрах хранилища доверенных сертификатов («CertStore») – тип хранилища и название соответствующего провайдера. При этом работа самой утилиты не изменилась. ЖТЯИ.00091-01 92 01. Правила пользования. п. 4.2. Старая редакция: « <Parameters inactiveTimeout=«60» checkInactiveTimeout=«30» serverSoTimeout=«600» /> <CertStore path=«c:\software\Keys\tomcat7\test_ca.store» password=«1» /> » Новая редакция: « <Parameters inactiveTimeout=«60» checkInactiveTimeout=«30» serverSoTimeout=«600» provider=”JCP” protocol=”GostTLS” /> <CertStore path=«c:\software\Keys\tomcat7\test_ca.store» password=«1» type=”CertStore” provider=”JCP” /> » Старая редакция: « Parameters: ... CertStore - хранилище доверенных сертификатов. path - путь к хранилищу, password - пароль к нему. » Новая редакция: « Parameters: ... provider – провайдер, реализующий работу с хранилищем, алгоритмом. protocol – протокол соединения. CertStore - хранилище доверенных сертификатов. path - путь к хранилищу, password - пароль к нему, type — тип хранилища, provider – провайдер, реализующий хранилище. »
14	Изменены наименование средства на СКЗИ «КриптоПро JCP» версия 2.0 R2 и децимальные номера на ЖТЯИ.00091-02.