

JaCarta для Linux

Руководство по внедрению

Аннотация

Настоящий документ представляет собой руководство по внедрению и использованию электронных ключей JaCarta с апплетом Laser в среде Linux. Электронные ключи JaCarta можно использовать в большинстве 32- и 64-битных операционных систем Linux.

Следование приведённым в настоящем документе инструкциям является верным, но не всегда единственно возможным способом достижения цели. В этом смысле эти инструкции носят рекомендательный характер.

Для эффективного внедрения и управления электронными ключами JaCarta в среде Linux требуется квалифицированный системный администратор.

Вопросы или пожелания по содержанию настоящего документа направляйте по адресу techwriters@aladdin-rd.ru.

Будем благодарны за конструктивные замечания и ответим на возникшие вопросы.

За технической поддержкой обращайтесь на веб-сайт ЗАО «Аладдин Р. Д.» по адресу <u>http://www.aladdin-rd.ru/support/index.php</u>.

Версия	2.0	
Редакция от	30.05.2014	
Листов	24	

Телефон +7 (495) 223-00-01 • Факс +7 (495) 646-64-40 • aladdin@aladdin-rd.ru • www.aladdin-rd.ru



Содержание

1.	Введение3
2.	Описание пакетов установки4
	2.1. Утилита с графическим интерфейсом4
	2.2. Утилита командной строки4
3.	Системные требования5
4.	Установка и примеры использования6
	4.1. Порядок установки6
	4.2. Предварительная установка библиотек для работы со смарт-картами и
	считывателями смарт-карт6
	4.3. Программное обеспечение с графическим интерфейсом8
	4.4. Консольная версия программного обеспечения16
5.	Настройка и использование JaCarta в Mozilla Firefox и Thunderbird18
	5.1. Подключение модуля PKCS#1118
	5.2. Настройка Mozilla Firefox для использования JaCarta при установлении
	SSL- и TLS-соединений20
	5.3. Пример использования21
6.	Список сокращений23
Лист	регистрации изменений24



1. Введение

Чтобы использовать электронные ключи JaCarta в среде Linux, необходимо установить:

- программное обеспечение, которое включает библиотеки, осуществляющие взаимодействие приложений с электронными ключами JaCarta через интерфейс PKCS#11;
- 2. ПО управления электронными ключами, которое позволяет изменять пароль пользователя, пароль администратора, пароль цифровой подписи и пароль разблокировки цифровой подписи электронных ключей JaCarta (см. табл. 1).

Табл. 1

Типы паролей электронных ключей JaCarta

Тип пароля	Описание
Пароль пользователя	Обеспечивает доступ к электронному ключу JaCarta на уровне пользователя.
Пароль администратора	Обеспечивает доступ к электронному ключу JaCarta на уровне администратора, в том числе позволяет разблокировать заблокированный пароль пользователя, кото- рый был заблокирован при превышении допустимого количества неверных попыток ввода.
Пароль цифровой подписи	Дополнительный пароль для использования цифровой подписи, который может быть назначен на этапе персонализации электронного ключа JaCarta.
Пароль разблокировки цифровой подписи	Позволяет разблокировать пароль цифровой подписи, который был заблокирован при превышении допустимого количества неверных попыток ввода.
-	

E

Подробное описание указанных выше паролей находится в документе «JC-Client. Руководство пользователя» и «JC-Client. Руководство администратора».

ПО управления электронными ключами представлена в двух вариантах:

- ПО с графическим пользовательским интерфейсом;
- утилита командной строки.

Установка программного обеспечения и использование электронных ключей JaCarta в среде Linux позволит осуществлять следующие действия:

- аутентификация пользователя по цифровому сертификату, хранящемуся в электронном ключе, при работе через браузер (в рамках протокола SSL/TLS);
- шифрование и цифровая подпись при использовании электронной почты;
- взаимодействие с другими приложениями, которые поддерживают интерфейс PKCS#11.



2. Описание пакетов установки

2.1. Утилита с графическим интерфейсом

Табл. 2

Пакеты установки утилиты с графическим интерфейсом

Имя файла	Описание
IDProtectClient610.12_ALT_x86.run	Сценарий установки ПО с графическим интерфейсом для использова- ния JaCarta в среде Linux для 32-битных платформ.
IDProtectClient610.12_ALT_x64.run	Сценарий установки ПО с графическим интерфейсом для использова- ния JaCarta в среде Linux для 64-битных платформ.



ПО с графическим интерфейсом работает как на 32-, так и на 64-битных версиях дистрибутивов, основанных на Debian и Red Hat.

2.2. Утилита командной строки

Табл. 3

Пакет установки консольной версии программного обеспечения

Имя файла	Описание
IDPClientDB_user.xml	Конфигурационный ХМL-файл.
aseInstall	Сценарий установки программного обеспечения для использования JaCarta в среде Linux.
IDPClientDB.xml	Конфигурационный ХМL-файл.
README	Файл справки (на английском языке).
ase-pin-tool	Утилита командной строки, позволяющая изменять пароль пользователя, пароль адми- нистратора, пароль цифровой подписи, пароль разблокировки цифровой подписи, а также выполнять другие операции.
libASEP11.so	Реализация интерфейса РКСS#11.

Утилита командной строки работает только на 32-битных версиях дистрибутивов, основанных на Red Hat.



3. Системные требования

Перед установкой программного обеспечения для использования электронных ключей JaCarta в среде Linux удостоверьтесь в том, что компьютер соответствует минимальным требованиям.

Табл. 4

Системные требования

Поддерживаемые операционные системы	 Дистрибутивы, основанные на Red Hat (32- и 64-битные платформы) Дистрибутивы, основанные на Debian (32- и 64-битные платформы) 	
Поддерживаемые браузеры	Firefox (версии 3 и более поздних версий)	
Поддерживаемые почтовые клиенты	Thunderbird (версии 3 и более поздних версий)	
Поддерживаемые модели электронных ключей	Смарт-карты и USB-токены JaCarta PKI, JaCarta FLASH, JaCarta FLASH/ГОСТ/PKI, JaCarta PRO/PKI и JaCarta ГОСТ/PKI	
Необходимые аппаратные средства	 USB-порт (для USB-токенов JaCarta) Считыватель смарт-карт (для смарт-карт JaCarta) 	
Необходимые драйверы и библиотеки	 Для CCID-совместимых считывателей и USB-токенов — драйвер CCID Для считывателей, не соответствующие спецификации CCID — драйверы для таких считывателей 	



В настоящем документе все действия описаны на примере дистрибутива ALT Linux 6/Astra Linux (кроме утилиты ase-pin-tool, стр. 16). Для других дистрибутивов указанные ниже команды и набор библиотек для работы со смарт-картами и считывателями смарт-карт могут отличаться. В таких случаях обращайтесь к справочным руководствам соответствующих дистрибутивов.



4. Установка и примеры использования

4.1. Порядок установки

Установка производится в два этапа:

- предварительная установка библиотек для взаимодействия операционной системы со смарт-картами и считывателями смарт-карт;
- 2. установка утилиты управления JaCarta.

4.2. Предварительная установка библиотек для работы со смарт-картами и считывателями смарт-карт

Для работы утилиты управления JaCarta необходимо установить следующие компоненты:

- PC/SC Lite промежуточный слой для обеспечения доступа к смарт-картам по стандарту PC/SC, пакет pcsc-lite.
- Библиотеки ccid и libusb для работы с USB-ключами, смарт-картами и считывателями смарт-карт.

Состав указанного выше ПО зависит от типов используемых устройств. Если будут использоваться и смарт-карты, и USB-токены, и при этом считыватель смарт-карт стандарта PC/SC не поддерживает CCID, то потребуется установить и драйвер считывателя, и драйвер CCID.



Для установки указанных библиотек в зависимости от используемой версии Linux выполните следующую команду (см. табл. 5 и рис. 1).

Табл. 5

Предварительная установка необходимых компонентов

ALT Linux 6	sudo apt-get install libusb pcsc-lite ccid
Astra Linux	sudo apt-get install libccid pcscd libpcsclite1

test@host-161: /home/test 📃 🗖	X
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка	
<pre>[test@host-161 ~]\$ sudo apt-get install libusb pcsc-lite ccid</pre>	6

Рис. 1 – Окно командной строки (терминала)





4.3. Программное обеспечение с графическим интерфейсом

УСТАНОВКА

Для установки ПО с графическим интерфейсом, выполните следующие действия:

- В домашней директории /home/user/, где user имя текущего пользователя, создайте любую директорию, например ID, и поместите в неё установочный пакет — IDProtectClient610.12_ALT_x86.run или IDProtectClient610.12_ALT_x64.run в зависимости от разрядности установленной операционной системы.
- 2. Параметру, определяющему права доступа пользователей к установочному пакету, присвойте значение 777, выполнив команду:
- sudo chmod 777 /home/user/ID/IDProtectClient610.12_ALT_x86.run
 - 3. Запустите установочный пакет командой:

sudo /home/user/ID/IDProtectClient610.12 ALT x86.run

4. В открывшемся окне нажмите кнопку Next (Далее).

S	etup (as superuser)
	Setup - IDProtectClient_ALT_x86
	Welcome to th IDProtectClient_ALT_x86 Setup Wizard.
	< Back Next > Cancel

Рис. 2 – Окно приветствия мастера установки

5. Укажите путь установки как показано на рисунке и нажмите кнопку Next (Далее).



Setup (as superuser)	
Installation Directory	athena Smartcard
Please specify the directory where IDProtectClient_ALT_x86 will b	e installed.
Installation Directory /opt/IDProtectClient-610.12	1
BitRock Installer - Sack Next :	Cancel

Рис. 3 – Путь установки

- 6. В зависимости от операционной системы выполните следующие действия.
 - Если вы устанавливаете ПО в операционной системе ALT Linux 6, переходите к шагу 7 настоящей процедуры.



• Если вы устанавливаете ПО в операционной системе Astra Linux, выберите компоненты устанавливаемого ПО (см. рис. 4 и табл. 6) и нажмите **Next** (Далее).

setup	
Select Components	athena Smartcard
Select the components you want t do not want to install. Click Next v	o install; clear the components you when you are ready to continue.
 ✗ Format ✗ Manager ✗ PINTool 	Click on a component to get a detailed description
BitRock Installer	< Back Next > Cancel

Рис. 4 – Выбор компонентов установки

Табл. 6

Компоненты установки

Компонент	Описание
Format	Утилита, позволяющая персонализировать электронные ключи JaCarta (подробнее см. документ «JC-Client. Руководство администратора»).
Manager	Утилита, позволяющая управлять сертификатами в памяти электронных ключей JaCarta (подробнее см. документ «JC-Client. Руководство администратора»).
PINTool	Утилита, позволяющая разблокировать и изменять пароль пользователя и пароль цифровой подписи JaCarta (подробнее см. документ «JC-Client. Руководство администратора»).



7. В открывшемся окне нажмите кнопку Next (Далее).

Setup (as superuser)	
Ready to Install	athena Smartcard
Setup is now ready to begin installing IDProtectClient_ALT_x8	б on your computer.
DisD = -[-T==+=]==	
< Back	lext > Cancel

Рис. 5 – Окно готовности к установке

Установка займёт некоторое время.

Setup (as superuser)	
Installing	athena Smartcard
Please wait while Setup installs IDProtectClient_ALT_x86 on	your computer.
Installing	
Creating uninstaller 25%	
BitRock Installer	
< Back	Nex Cancel

Рис. 6 – Процесс установки

8. По завершении установки нажмите кнопку **Finish** (Готово), после чего дождитесь перезагрузки компьютера.





Рис. 7 – Окно завершения установки

ПРОВЕРКА РАБОТОСПОСОБНОСТИ

Чтобы убедится в том, что установка прошла успешно, выполните следующие действия.

- 1. Подсоедините электронный ключ JaCarta к компьютеру.
- 2. В зависимости от используемой версии Linux запустите установленное приложение следующим способом (см. табл. 7)

Табл. 7

Запуск установленного приложения

ALT Linux 6	В меню Applications (Приложения) выберите Other (Прочие) > IDProtect PINTool (см. рис. 8).
Astra Linux	Из стартового меню выберите Прочие > IDProtect PINTool (см. рис. 9).





Рис. 8 – Запуск приложения управления электронными ключами JaCarta (на примере ALT Linux 6)



Рис. 9 - Запуск приложения управления электронными ключами JaCarta (на примере Astra Linux)



3. Убедитесь, что в приложении отображается подключенное устройство JaCarta.

Applications	Places	System 🔛	1			Thu Sep 27,	5:20 PM 🗖
Computer			IDProt	ect PINTool			
	JaCa	rta#0B5200	1821209243				
grinch's Hom	Р	IN Type		Status			
Trash	9 <u>#</u>	IN	0	Valid	Change		
	Ls	ignature	•	Absent		_	
Screenshots							
					Close		

Рис. 10 – Окно приложения управления электронными ключами JaCarta

ПРИМЕР ИСПОЛЬЗОВАНИЯ

- 1. Запустите установленное приложение (см. п. «Проверка работоспособности»).
- 2. В открывшемся окне щёлкните Change (Изменить).

Computer		C	IDProt	ect PINTool			
ŝ	Ja	Carta#0B5200	1821209243				
grinch's Hom		PIN Type		Status			
Trash	推	PIN	0	Valid	Change		
	L	Signature	•	Absent		_	
Screenshots						100	
					Close		

Рис. 11 – Окно приложения управления электронными ключами JaCarta

3. В следующем окне в поля Current user pin (Текущий пароль пользователя), New user pin (Новый пароль пользователя), Confirm new pin (Подтверждение нового паро-



ля) введите соответственно текущий пароль пользователя JaCarta, новый пароль пользователя JaCarta и подтверждение нового пароля пользователя JaCarta, после чего нажмите кнопку **Change** (Изменить).

C Applications	Places Sy	stem 🔤 🍪 🕤 🕮	Thu Sep 27, 5:35 PM 📃
Computer	1.5.4	IDProtect PINTool	
	Jacarta	IDProtect Change User PIN 🛛 🔍	
grinch's Hom	PIN	JaCarta#0B52001821209243	
Trash	T PIN	Enter Your User Pin Current User Pin	
	L Sign	New User PIN ********* Confirme New PIN *********	
Screenshots		*	
		Close Chynge	

Рис. 12 – Смена пароля пользователя электронного ключа JaCarta

4. В отобразившемся окне нажмите ОК.

Computer		IDProtect PINTool	_ X
	JaCarta#0B5200	1821209243	
grinch's Hom	PIN Type	Status	
Trash	<u>非</u> pin	IDProtectPINTool X	Change
	/ Signature	<u>Seo</u> k	
Screenshots			
			Close

Рис. 13 – Подтверждение смены пароля пользователя электронного ключа JaCarta



4.4. Консольная версия программного обеспечения

УСТАНОВКА

Чтобы установить консольную версию ПО для использования JaCarta в среде Linux, выполните следующие действия.

- 1. Скопируйте файлы дистрибутива в любую папку на жёстком диске.
- 2. В командной строке из папки с файлами библиотеки выполните сценарий **aseInstall**, используя следующую команду:
- sh aseInstall
 - Убедитесь в отсутствии сообщений об ошибках (кроме случаев обновления, когда отображаются сообщения о существовании ранее установленных файлов — такие сообщения можно игнорировать).

Утилита работает только на 32-битных версиях Linux-дистрибутивов, основанных на Red Hat.

ПРОВЕРКА РАБОТОСПОСОБНОСТИ

В состав дистрибутива ПО входит утилита командной строки **ase-pin-tool.** Данная утилита позволяет изменять пароль пользователя JaCarta, пароль администратора JaCarta, пароль цифровой подписи, пароль разблокировки цифровой подписи. Описание параметров этой утилиты приведено в табл. 8.

Табл. 8

Параметры утилиты командной строки ase-pin-tool

Параметр	Описание
-1	Отображает список доступных считывателей.
-r	Позволяет задать активный считыватель.
-u	Позволяет изменить пароль пользователя. Допускаются только символы из набора ASCII. Если пароль пользователя заблокирован, сначала необходимо ввести пароль администратора.
-а	Позволяет задать пароль администратора JaCarta. Допускаются только символы из набора ASCII.
-d	Позволяет изменить пароль цифровой подписи. Допускаются только символы из набора ASCII. Если пароль цифровой подписи заблокирован, сначала необходимо ввести пароль разблокировки цифровой подписи.
-р	Позволяет изменить пароль разблокировки цифровой подписи. Допускаются только символы из набора ASCII.
-h	Отображает справку по использованию утилиты командной строки ase-pin-tool (на английском языке).



ПРИМЕР ИСПОЛЬЗОВАНИЯ

- 1. Подсоедините JaCarta к компьютеру.
- 2. Выполните следующую команду:
- ase-pkcs-tool -u
 - Отобразится следующая строка:
- Current User PIN:
 - 3. Введите текущий пароль пользователя и нажмите клавишу ВВОД.
 - Отобразится строка для ввода нового пароля пользователя:
- New User PIN:
 - 4. Введите новый пароль пользователя и нажмите клавишу ВВОД. Отобразится строка подтверждения нового пароля пользователя:
- Confirm New User PIN:
 - Подтвердите новый пароль пользователя и нажмите клавишу ВВОД.
 В случае успешной смены пароля пользователя отобразится следующее сообщение:

Program Succeeded



5. Настройка и использование JaCarta в Mozilla Firefox и Thunderbird

Для доступа к защищённому сайту с электронным ключом JaCarta можно использовать браузер Mozilla Firefox. Для этого необходимо выполнить следующие действия:

- подключить к Mozilla Firefox модуль PKCS#11 из состава установочного пакета;
- настроить Mozilla Firefox на использование JaCarta при установлении SSL- и TLS-соединений (требуется для Firefox 4.0 и более поздних версий).

Для шифрования, формирования и проверки подписи сообщений электронной почты с электронным ключом JaCarta можно использовать приложение Mozilla Thunderbird. Для этого необходимо подключить к Mozilla Thunderbird модуль PKCS#11.

5.1. Подключение модуля PKCS#11

Чтобы использовать электронные ключи JaCarta с браузером Mozilla Firefox или почтовым клиентом Mozilla Thunderbird по интерфейсу PKCS#11, в настройках соответствующего приложения укажите путь к файлу **libASEP11.so** из состава ПО.



Ниже рассматривается подключение модуля PKCS#11 к Mozilla Firefox. Подключение его к Mozilla Thunderbird осуществляется по аналогичной процедуре.

Для подключения модуля PKCS#11 к браузеру Mozilla Firefox выполните следующие действия.

- 1. В главном меню браузера Mozilla Firefox выберите **Правка > Настройки**.
- 2. В отобразившемся окне щёлкните на значке 🍄 (раздел Дополнительные).
- **3.** Выберите вкладку **Шифрование** и нажмите **Устройства защиты**.



Отобразится следующее окно.

ние устройствами 🛛 🗛 🗆 🗙
Подробно Значе На <u>ч</u> ать сеанс Зак <u>о</u> нчить сеанс Сменить п <u>а</u> роль За <u>г</u> рузить В <u>ы</u> грузить Использовать <u>F</u> IPS
T

Рис. 14 – Окно Управление устройствами

4. Нажмите Загрузить.

Отобразится следующее окно.

🥹 Загрузка устройства РКСЅ#11 _		×				
Введите информацию о модуле, который вы хотите добавить.						
И <u>м</u> я модуля: New PKCS#11 Module						
Имя <u>ф</u> айла модуля: О <u>б</u> зо	p					
Отмена О	к					

Рис. 15 – Окно Загрузка устройства

- 5. В поле Имя модуля задайте отображаемое имя (например, «JaCarta»).
- 6. В поле Имя файла модуля укажите путь к файлу libASEP11.so из состава ПО для использования JaCarta в среде Linux. При необходимости воспользуйтесь кнопкой Обзор.
- 7. Нажмите ок.



Информация о подсоединённом электронном ключе JaCarta отобразится в окне управления устройствами.

6) Управле	ение устройств	зами	_ = ×		
	Модули и устройства за	Подробно Значе		На <u>ч</u> ать сеанс		
	▼NSS Internal PKCS #11 Module Общ. криптослужбы Модуль защиты ▼Модуль встроенных корне Builtin Object Token ▼JaCarta JaCarta#0953000516284	Состояние Описание	He зарег Athena A	Закончить сеанс		
		Модуль защиты ▼Модуль встроенных корне Builtin Object Token ▼JaCarta JaCarta#0953000516284	Модуль защиты Изготовит Athena дуль встроенных корне Версия HW 1.0 Builtin Object Token Версия FW 1.0 Зага Асата	Athena S 1.0	Сменить пароль	
				1.0 IaCarta#0	За <u>г</u> рузить	
			JaCarta#0953000516284	JaCarta#0953000516284	JaCarta#0953000516284	JaCarta#0953000516284 Изготовит А
		Версия НW	1.0	Использовать <u>F</u> IPS		
		Версия FW	2.0	•		
				ОК		

Рис. 16 — Информация о подсоединённом электронном ключе JaCarta в окне управления устройствами Здесь также можно поменять пароль пользователя подсоединённого электронного ключа JaCarta, воспользовавшись кнопкой Сменить пароль.

8. Чтобы закрыть окно управления устройствами, нажмите **ОК.**

5.2. Настройка Mozilla Firefox для использования JaCarta при установлении SSL- и TLSсоединений

Чтобы обеспечить возможность доступа к защищённым сайтам по протоколам SSL и TLS с использованием закрытого ключа и цифрового сертификата в памяти JaCarta, выполните следующие действия.



Данные действия необязательны для Firefox версий до 4.0.

- **1.** Запустите Mozilla Firefox.
- 2. В адресной строке наберите about:config и нажмите клавишу ВВОД. В окне браузера отобразится предупреждающее сообщение.
- 3. Щёлкните на кнопке Я обещаю, что буду осторожен.



Окно браузера примет следующий вид.

Firefox 🔻				
about:config	+			
♦ → about:config				2
Фильтр:				
Имя настройки		Состояние	Тип	Значение
accelerometer.enabled		по умолчанию	логическ	true
accessibility.accesskeycausesactivation		по умолчанию	логическ	true
accessibility.blockautorefresh		по умолчанию	логическ	false
accessibility.browsewithcaret		по умолчанию	логическ	false
accessibility.browsewithcaret_shortcut.enabled		по умолчанию	логическ	true
accessibility.mouse_focuses_formcontrol		по умолчанию	логическ	false
accessibility.tabfocus		по умолчанию	целое	7
accessibility.tabfocus_applies_to_xul		по умолчанию	логическ	false

Рис. 17 – Список настроек Mozilla Firefox

4 . Найдите настройку

security.ssl.allow_unrestricted_renego_everywhere__temporari ly_available_pref (для быстрого поиска настройки введите или скопируйте её имя в поле Фильтр).

5. Если она имеет значение false (ложь), двойным щелчком присвойте ей значение true (истина).

5.3. Пример использования

Чтобы получить доступ к защищённому сайту с использованием браузера Mozilla Firefox и электронного ключа JaCarta, выполните следующие действия.

- 1. Убедитесь в том, что к компьютеру подсоединён электронный ключ JaCarta.
- 2. Запустите браузер Mozilla Firefox.
- В адресной строке введите адрес защищенного сайта (адрес должен начинаться с https://) и нажмите клавишу ВВОД.
 Отобразится следующее окно.

Требуется пароль		
?	Введите мастер-пароль для доступа в JaCarta	
	ОК Отмена	

Рис. 18 – Окно ввода пароля пользователя электронного ключа JaCarta

4. Введите пароль пользователя электронного ключа JaCarta и нажмите **ОК**.



Отобразится следующее окно.



Рис. 19 – Окно идентификации пользователя

5. Установите флажок Запомнить это решение и нажмите ОК. Защищённая страница отобразится в окне браузера.



6. Список сокращений

- ОС операционная система
- ПО Программное обеспечение
- SSL Secure Socket Layer (Безопасный сокет и уровень)
- TLS Transport Layer Security (Протокол TLS)

PKCS – Public Key Cryptography Standards (Стандарты криптографии с открытым ключом)

PC/SC — Personal Computer/Smart Card (Персональный компьютер/смарт-карта), набор спецификаций для доступа к смарт-картам

ASCII – American Standard Code for Information Interchange (Американский стандартный код для обмена информацией)

CCID – Chip/Smart Card Interface Devices.



Лист регистрации изменений

Версия документа	Изменения
1.0	Исходная версия документа.
2.0	Добавлены сведение об установке на Astra Linux.



Телефон: +7 (495) 223-00-01 Факс: +7 (495) 646-64-40 aladdin@aladdin-rd.ru

www.aladdin-rd.ru

ий документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодатель ством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ЗАО «Аладдин Р. Д.». Использование этих материалов любым

особом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. ция, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их ии, характеристики, версии, доступность и пр. могут быть изменены компанией «Аладдин Р. Д.» без предварительного уведомления. В данном документе компания «Аладдин Р. Д.» не предоставляет никаких ни явных, ни подразумеваемых гарантий.

Владельцем товарных знаков Аладдин, Aladdin, JaCarta, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствую щие продукты является ЗАО «Аладдин Р. Д.».

Владельцем товарных знаков Apple, iPad, iPhone, Mac OS, OS X является корпорация Apple Inc. Владельцем товарного знака IOS является компания Cisco (Cisco Systems, Inc). Владельцем товарного знака Windows Vista и др. — корпорация Microsoft (Microsoft Corporation). Названия прочих технологий, продуктов, комп упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев.

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (бессрочно), № 2874 от 18.05.12 Microsoft Silver OEM Hardware Partner, Oracle Gold Partner, Apple Developer

Лицензия ФСБ России № 12632 Н от 20.12.12

É Developer Microsoft Partner

Сертификат соответствия СМК ГОСТ Р ИСО 9001-2011



1

© ЗАО «Аладдин Р. Д.», 1995—2014 Все права зашишены

V2.0 30.05.2014

стр. 24 из 24