**Приложение 1.**

ОС, поддерживаемые СКЗИ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Windows** | **Linux** | **FreeBSD** | **Solaris** | **iOS** | **Mac OS** |
| КриптоПро CSP 3.6.1 | Windows 2000 (ia32)Windows XP/2003/Vista/2008/7/2008R2 (ia32, ia64, x64) | ALT Linux (ia32, x64);Debian (ia32, х64);Trustverse Linux XP (ia32);**Linux Standard Base ISO/IEC 23360 (ia32, x64):**Cent OS (ia32, x64)Fedora (ia32, x64)Linpus (ia32)Mandriva (ia32, x64)MontaVista Linux (ia32, x64)Oracle Enterprise Linux (ia32, x64)Оpen SUSE (ia32, x64)Red Hat Enterprise Linux (ia32, x64)SUSE Linux Enterprise (ia32, x64)SUSE LINUX (ia32)Ubuntu (ia32, x64)Xandros (ia32) | FreeBSD 7/8/9 (ia32, x64) | Solaris 10/11 (sparc, ia32, x64) | Apple iOS (ARM)(только для КС1) | Mac OS X (x64)(только для КС1) |
| ViPNet CSP 3.2 | Microsoft XP SP3 (32-разрядная)Server 2003 (32-разрядная)Vista SP2 (32/64-разрядная)Windows 7 (32/64-разрядная)Windows Server 2008 (32/64-разрядная)Windows Server 2008 R2 (64-разрядная) | SuSe Linux Enterprise Server 10Slackware Linux 12.0RedHat Enterprise Linux 4SuSe Linux Enterprise Server 10 SP1,SP2, SuSe Linux 10.0Slackware Linux 10.2Ubuntu 8.04 LTS DesktopDebian Etch 4.0 r1 Linux XP 2008 Server Linux XP 2008 Desktop Secure EditionOpen SuSe Linux 11.1 | - | - | - | - |
| С-терра CSP VPN Client 3.11  | Windows XP Professional, Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows Server 2003, Microsoft Windows Server 2008 | Red Hat Enterprise Linux 5 (в том числе производные варианты ОС - CentOS 5, Crossbeam Systems Linux 9)  | - | - | - | - |
| Континент-АП 3.6 | Windows XP Professional SP3 x86 Windows 2003 Server SP2 x86/x64 Windows 2003 Server R2 SP2 x64 Windows Vista SP2 x86/x64 (кроме всех выпусков Starter и Home Edition) Windows 2008 Server SP2 x86/x64Windows 2008 Server R2 SP1 x64Windows 7 SP1 x86/x64 (кроме всех выпусков Starter и Home Edition) | Альт Линукс СПТ 6.0 Рабочая станция x86/x64 Альт Линукс СПТ 6.0 Сервер x86/x64 Mandriva Spring 2008.1 x86 | - | - | - | - |
| StoneGate Firewall/ VPN Client 5 | Windows XP,Windows Vista (32, 64 bit), Windows 7 (32, 64 bit), Windows 8 (32, 64 bit) | - | - | - | - | - |
| StoneGate SSL VPN Access Client | Windows 2000, Windows XP, Windows 2003 Server, Windows Vista (32, 64 bit), Windows 7 (32, 64 bit) | Linux (32, 64 bit) |  |  |  |  |
| VipNet Client 3.1 | Windows 2000/XP/Server 2003/Vista/Server 2008 | - | - | - | - | - |
| VipNet Client iOS | - | - | - | - | версии 4.2.х, 4.3.2, 4.3.3 — для iPad 1, iPhone 3G, iPhone 3GS, iPhone 4; версия 4.3.3 — для iPad 2; версия 5.0.1 — для iPad 2, iPhone 4S; версия 5.1.1 — для iPad 1, iPad 2, iPhone 4, iPhone 4S, iPhone 3GS | - |

СЗИ от НСД, которые необходимо использовать для классов больших чем КС1 ( для КС2-КС3)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Аккорд-АМДЗ** | **Соболь** | **КРИПТОН-ЗАМОК/У** | **МАРШ!** |
| КриптоПро CSP 3.6.1(исполнение 2) | Только для Windows4012-006-11443195-2005 ТУ | 2.1УВАЛ.00300-58-01 ТУ3.0RU.40308570.501410.001 ПС | КБДЖ.468243.067 ТУ | - |
| ViPNet CSP 3.2 | - | 2.1УВАЛ.00300-58-01 ТУ3.0RU.40308570.501410.001 ПС | - | - |
| С-терра CSP VPN Client 3.11(для КС2 – КС3) | 4012-006-11443195-2005 ТУ | 2.1УВАЛ.00300-58-01 ТУ3.0RU.40308570.501410.001 | модификации М-526А, М-526Б, М-526В, М-526Е | СПДС-USB-01ТУ 4024-001-70221576-2011 |
| Континент-АП 3.6 | - | 2.1УВАЛ.00300-58-01 ТУ3.0RU.40308570.501410.001 | - | - |
| StoneGate Firewall/ VPN Client 5 | 4012-006-11443195-2005 ТУ | 2.1УВАЛ.00300-58-01 ТУ3.0RU.40308570.501410.001 | КБДЖ.468243.067 ТУ | МАРШ!-USBТУ 4024-033-11443195-2010 |
| StoneGate SSL VPN Access Client | 4012-006-11443195-2005 ТУ | 2.1УВАЛ.00300-58-01 ТУ3.0RU.40308570.501410.001 | - | МАРШ!-USBТУ 4024-033-11443195-2010 |
| VipNet Client 3.1 | АПМДЗ «Аккорд 3.2» | электронный замок «Соболь 2.1» | - | - |

Итоговая сводная таблица по клиентам Remote VPN (не шлюзам)

| **Техническое решение Remote VPN, сертифицированное ФСБ Р** | **Операционные системы, для работы в которых сертифицировано решение и максимальный класс криптозащиты** |
| --- | --- |
| **Наименование, версия, № формуляра** | **Используется CSP и учитываются его ограничения** | **Используемое средство защиты доступа, сертифицированное ФСБ** | **Windows XP** | **Windows Vista / 7** | **Windows 8** | **Windows 2003/2008** | **Linux** | **FreeBSD** | **Solaris** | **Mac OS X** | **Apple iOS** |
| CSP VPN Client 3.11РЛКЕ.00005-02 30 01 | КриптоПро CSP 3.6 | - | КС1 | КС1 | - | КС1 | - | - | - | - | - |
| Аккорд-АМДЗ | КС2 | КС2 | - | КС2 | - | - | - | - | - |
| Соболь 2.1 или 3.0 | КС2 | КС2 | - | КС2 | - | - | - | - | - |
| КРИПТОН-ЗАМОК/У | КС2 | КС2 | - | КС2 | - | - | - | - | - |
| МАРШ! | -15 | -15 | - | -15 | - | - | - | - | - |
| Континент-АП 3.6RU.88338853.501430.002 30 | КриптоПро CSP 3.6 R2 и 3.6.1 | - | КС1 | КС1 | - | КС1 | КС1 | - | - | - | - |
| Соболь 2.1 или 3.0 | КС2 | КС2 | - | КС2 | КС2 | - | - | - | - |
| StoneGate Firewall/ VPN Client 589625543.4012-001 30 02 | КриптоПро CSP 3.6.1 | - | КС1 | КС1 | КС1 | - | - | - | - | - | - |
| Аккорд-АМДЗ | КС2 | КС2 | КС2 | - | - | - | - | - | - |
| Соболь 2.1 или 3.0 | КС2 | КС2 | КС2 | - | - | - | - | - | - |
| КРИПТОН-ЗАМОК/У | КС2 | КС2 | КС2 | - | - | - | - | - | - |
| МАРШ! | -15 | -15 | -15 | - | - | - | - | - | - |
| StoneGate SSL VPN Access Client 89625543.4012-003 30 02 | КриптоПро CSP 3.6 R2Валидата CSP 4.0 | - | КС1 | КС1 | - | КС1 | КС1 | - | - | - | - |
| Аккорд-АМДЗ | КС2 | КС2 | - | КС2 | КС2 | - | - | - | - |
| Соболь 2.1 или 3.0 | КС2 | КС2 | - | КС2 | КС2 | - | - | - | - |
| МАРШ! | -15 | -15 | - | -15 | КС2 | - | - | - | - |
| VipNet Client 3.1ФРКЕ. 00004-04 30 01 | VipNet. Криптопровадер | - | КС1 | КС1 (только Vista) | - | КС1 | - | - | - | - | - |
| Аккорд-АМДЗ | КС2 | КС2 | - | КС2 | - | - | - | - | - |
| Соболь 2.1 | КС2 | КС2 | - | КС2 | - | - | - | - | - |
| VipNet Client 3.1 КС3ФРКЕ.00063-04 30 01 | VipNet. Криптопровадер | Аккорд-АМДЗ | КС3 | КС3 | - | КС3 | - | - | - | - | - |
| Соболь 2.1 | КС3 | КС3 | - | КС3 | - | - | - | - | - |
| VipNet Client iOS ФРКЕ.00072-02 30 01 | ? | - | - | - | - | - | - | - | - | - | КС1 |
| КриптоПро CSP 3.6.1ЖТЯИ.00050-03 30 01 | - | - | КС1 | КС1 | КС1 | КС1 | КС1 | КС1 | КС1 | КС1 | КС1[[1]](#footnote-1) |
| Аккорд-АМДЗ | КС3 | КС2 | КС2 | КС3 | КС2 | КС2 | КС2 | КС1 | КС11 |
| Соболь 2.1 или 3.0 | КС3 | КС2 | КС2 | КС3 | КС2 | КС2 | КС2 | КС1 | КС11 |
| КРИПТОН-ЗАМОК/У | КС3 | КС2 | КС2 | КС3 | КС2 | КС2 | КС2 | КС1 | КС11 |
| VipNet CSP 3.2ФРКЕ.00061-01-30 01 | - | - | КС1 | КС1 | - | КС1 | КС1 | - | - | - | - |
| Соболь 2.1 или 3.0 | КС2 | КС2 | - | КС2 | КС2 | - | - | - | - |

**Приложение2.**

Наиболее интересные ограничения и условия

1. **Криптопро CSP 3.6.1** Формуляр ЖТЯИ.00050-03 30 01.

*“1.2 Эксплуатация СКЗИ ЖТЯИ.00050-03 должна проводиться в соответствии с эксплуатационной документацией, предусмотренной настоящим Формуляром*

*1.4 При эксплуатации СКЗИ ЖТЯИ.00050-03 должны использоваться сертификаты открытых ключей, выпущенные Удостоверяющим центром, сертифицированным по классу защиты не ниже класса защиты используемого СКЗИ.”*

1. **Криптопро CSP 3.6.1** Формуляр ЖТЯИ.00050-03 30 01.

*“1.5 При встраивании СКЗИ ЖТЯИ.00050-03 в прикладные системы необходимо проводить оценку влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к СКЗИ требований:*

*- для исполнения 3 (класс защиты КС3) – во всех случаях;*

*- для исполнений 1 (класс защиты КС1) и 2 (класс защиты КС2) - в следующих случаях:*

*1) если информация, обрабатываемая СКЗИ, подлежит защите в соответствии с законодательством Российской Федерации;*

*2) при организации защиты информации, обрабатываемой СКЗИ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;”*

1. **Криптопро CSP 3.6.1** Формуляр ЖТЯИ.00050-03 30 01.

*“7.8 При эксплуатации СКЗИ ЖТЯИ.00050-03 должны соблюдаться следующие сроки использования пользовательских закрытых ключей и сертификатов: максимальный срок действия закрытого ключа ЭП (ключа ЭП) - 1 год 3 месяца;*

*Допускается хранение закрытых ключей на HDD ПЭВМ (в реестре ОС Windows, в разделе HDD при работе под управлением других ОС) при условии распространения на HDD или на ПЭВМ с HDD требований по обращению с ключевыми носителями.”*

1. **Криптопро CSP 3.6.1** Руководство администратора. Часть 16. ЖТЯИ.00050-03 90 02

*“16. Должна быть запрещена работа СКЗИ при включенных в ПЭВМ штатных средствах выхода в радиоканал*

*20. ЗАПРЕЩАЕТСЯ использование беспроводных клавиатур и компьютерных мышей”*

1. **Криптопро CSP 3.6.1** Руководство администратора. Часть 16. ЖТЯИ.00050-03 90 02

*“17. При функционировании исполнения 2 СКЗИ в программно-аппаратных средах Windows XP/2003 , ОС Solaris 9/10 (sparc, ia32, x64) инициализация ПДСЧ должна производиться с использованием внешней гаммы.”*

1. **Криптопро CSP 3.6.1** Руководство администратора безопасности. Использование СКЗИ под управлением ОС iOS. ЖТЯИ.00050-03 90 02-07

*“2. Для операционной системы iOS КриптоПро CSP не поставляется в виде конечного приложения. КриптоПро CSP для iOS представляет собой фреймворк для разработки, который содержит в себе объектный файл, реализующий функции CSP, ресурсы и заголовочные файлы. Фреймворк не имеет механизма самостоятельной установки в операционную систему. Установка осуществляется в составе прикладной программы, разработанной на основе фреймворка теми средствами, которые предлагает разработчик прикладной программы.*

1. **Криптопро CSP 3.6.1** Руководство администратора безопасности. Использование СКЗИ под управлением ОС iOS. ЖТЯИ.00050-03 90 02-07

*10. Ежесуточная перезагрузка ПЭВМ.*

*15. Должна быть запрещена работа СКЗИ при включенных в ПЭВМ штатных средствах выхода в радиоканал.”*

1. **КриптоПро УЦ.** Формуляр. ЖТЯИ.00067-02 30 01.

*“3. Межсетевой экран должен быть сертифицирован ФСБ России на соответствие требованиям к устройствам типа межсетевой экран по 4 классу защищенности. Не входит в комплект поставки, поставляется по согласованию с заказчиком.”*

1. **С-терра CSP VPN Client 3.11** Правила пользования РЛКЕ.00005-02 90 02.

*“4.5…. Для всех исполнений СКЗИ для исключения возможности влияния аппаратных компонентов СФК на функционирование СКЗИ должны быть выполнены следующие требования:*

*в случае обработки информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, необходимо проводить исследования ПО BIOS СВТ, на котором установлен ПК "CSP VPN Gate", на соответствие требованиям "Временных методических рекомендаций к проведению исследований программного обеспечения BIOS по документированным возможностям"*

1. **С-терра CSP VPN Client 3.11** Правила пользования РЛКЕ.00005-02 90 02.

*“4.7 Требования к обращению с ключевыми документами*

*Требования к ключам регламентируются документом «Руководство администратора безопасности» КриптоПро CSP, согласно которому срок действия открытых и закрытых ключей шифрования – 1 год 3 месяца.”*

1. **StoneGate Firewall/ VPN Client 5.** Программный комплекс криптографической защиты «StoneGate Firewall/VPN» версия 5 ПРАВИЛА ПОЛЬЗОВАНИЯ 89625543.4012-001 90 02

*“6. …. Аутентификация пользователей при обращении к шлюзу StoneGate Firewall/VPN возможна с использованием метода аутентификации на основе сертификатов. Возможна комбинация методов аутентификации по сертификатам c другими методами для предоставления пользователю доступа к функциям системы.*

*Аутентификация абонентов при взаимодействии шлюза StoneGate Firewall/VPN с другими шлюзами возможна с использованием методов аутентификации на основе сертификатов и на основе предварительно распределяемых ключей. При использовании метода аутентификации на основе предварительно распределяемых ключей каждая пара шлюзов должна иметь уникальный ключ длиной 256 бит (при использовании для генерирования и распределения ключей для шлюзов StoneGate Firewall/VPN функций системы управления SMC это требование выполняется автоматически)*

*При использовании для аутентификации абонентов сертификатов, требования к аутентификации аналогичны предъявляемым при функционировании соответствующих используемых в комплексе StoneGate Firewall/VPN исполнений СКЗИ «КриптоПро CSP 3.6.1».* *При использовании иных методов аутентификации требования к аутентификации определяются настоящими Правилами.*

1. **StoneGate Firewall/ VPN Client 5.** Программный комплекс криптографической защиты «StoneGate Firewall/VPN» версия 5 ПРАВИЛА ПОЛЬЗОВАНИЯ 89625543.4012-001 90 02

*“6. Если с помощью StoneGate Firewall/VPN обрабатывается информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, должно быть обеспечено соответствие ПО BIOS СВТ оператора такой информации (включая оператора персональных данных), на котором установлены компоненты комплекса, «Временным методическим рекомендациям к проведению исследований программного обеспечения BIOS по документированным возможностям». Проверка соответствия ПО BIOS СВТ субъекта данных (например, субъекта персональных данных) не требуется, но рекомендуется”*

1. **StoneGate Firewall/ VPN Client 5.** Программный комплекс криптографической защиты «StoneGate Firewall/VPN» версия 5 ПРАВИЛА ПОЛЬЗОВАНИЯ 89625543.4012-001 90 02

*“6.1 …*

*- при использовании СКЗИ на ПЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей должны использоваться дополнительные методы и средства защиты (межсетевые экраны). При этом возможно задействовать функции разграничения сетевого доступа шлюза StoneGate Firewall/VPN (данный функционал имеет сертификат ФСТЭК);”*

1. **Криптопро CSP 3.6.1** Руководство администратора. Часть 16. ЖТЯИ.00050-03 90 02

*“15....* *при использовании СКЗИ на ПЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN сетей и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.”*

1. **МАРШ!**

*В настоящее время производитель устанавливает на МАРШ! только Linux. Идет тестирование Windows Embeded. Если МАРШ! будет поставляться в составе с Windows, то условия формуляра позволяют использовать такой вариант для класса КС2*

**Приложение 3.**

Типовой комплект документов при использовании сертифицированных СКЗИ для защиты ПДн (ссылки на пункты типовых требований149/6/6-622 ФСБ России по защите ПДн, которые в свою очередь скопированы из приказа 152 ФАПСИ):

* заключение о возможности эксплуатации криптосредств (п. 2.3);
* журнал учета используемых криптосредств (п. 3.4);
* журнал учета технической документации к криптосредствам (п. 3.4);
* приказ о назначении лиц (пользователей криптосредств), допущенных к работе с криптосредствами (п. 2.3);
* документ, устанавливающего порядок обеспечения безопасности ПДн при помощи криптосредств (п. 1.3);
* документ, устанавливающего порядок организации контроля за соблюдением условий использования криптосредств (п. 2.3);
* приказ о назначении ответственного пользователя криптосредств (п. 2.6);
* описание функциональных обязанностей ответственного пользователя криптосредств  (п. 2.7);
* лицевые счета на пользователей криптосредств (п. 3.5);
* технический (аппаратный) журнал регистрации разовых ключевых носителей  (п. 3.6);
* приказ о назначении комиссии по уничтожению ключевых документов (п. 3.22);
* документ, устанавливающий требования к режимным помещениям, в которых эксплуатируются криптосредства (п. 4.1);
* журнал учета хранилищ (п. 4.5);
* журнал проверок исправности сигнализации (п. 4.7);
* журнал учета ключей от хранилищ ключевых документов и технической документации (п. 4.8);
* журнал службы охраны (п. 4.9).

[Читать полную версию статьи на сайте Sec.ru](http://daily.sec.ru/publication.cfm?pid=41291)

*Источник: Sec.ru*

1. Только в составе прикладного ПО [↑](#footnote-ref-1)