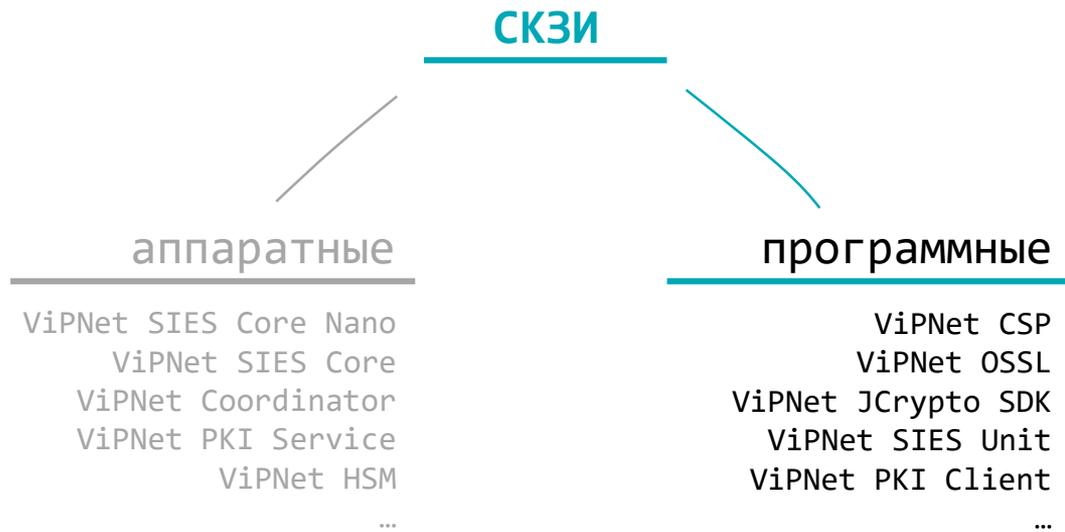


Что нужно знать при использовании СКЗИ

Арина Эм
Александр Бодров

СКЗИ от Инфотекса

Аппаратные и программные СКЗИ



Вопросы, которые сегодня обсудим

- Где использовать?
- Как передавать?
- Что делать, если филиал за рубежом?
- Кому эксплуатировать?
- Как учитывать?
- Нужна ли оценка влияния?
- Зачем все это?

Расскажите нам

Какие вопросы вам задавали на местах?



Где использовать?

Ищем ответ в Правилах пользования



Правила пользования ViPNet CSP 4.4



ViPNet CSP при выполнении требований, изложенных в настоящих правилах пользования и другой эксплуатационной документации, обеспечивает защиту информации, не содержащей сведений, составляющих государственную тайну.



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4702 от "28" декабря 2023 г.

Действителен до "28" декабря 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) ViPNet CSP 4.4 (Версия 4.4.8) (исполнения: 1, 2, 3, 4, 5, 6) в комплектации согласно формуляру ФРКЕ.00106-09 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнений: 1, 4), класса КС2 (для исполнений: 2, 5), класса КС3 (для исполнений: 3, 6), Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнений: 1, 4), класса КС2 (для исполнений: 2, 5), класса КС3 (для исполнений: 3, 6), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции №№ 637Д-000518, 637Д-000519.

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00106-09 30 01 ФО.

И в сертификате



Сертификат ViPNet CSP 4.4

Всё, что не ГТ – в перечне

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
Государственная тайна	Статья 5 Закона РФ от 21.07.1993 N 5485-1 "О государственной тайне"
	Указ Президента РФ от 30.11.1995 N 1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне"
	Статья 5, 9 Федерального закона от 09.02.2007 N 16-ФЗ "О транспортной безопасности"
	Статья 12 Федерального закона от 12.08.1995 N 144-ФЗ "Об оперативно-розыскной деятельности"
	Статьи 17, 19 Федерального закона от 03.04.1995 N 40-ФЗ "О федеральной службе безопасности"
	Статья 26 Федерального закона от 03.07.2016 N 226-ФЗ "О войсках национальной гвардии Российской Федерации"
Коммерческая тайна	Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне"
	Статья 14.7 Федерального закона от 26.07.2006 N 135-ФЗ "О защите конкуренции"
	Статья 12 Федерального закона от 28.11.2011 N 335-ФЗ "Об инвестиционном товариществе"
Конфиденциальная информация, полученная в ходе переговоров о заключении договора от другой стороны	Статья 434.1 Гражданского кодекса РФ (часть первая)
Конфиденциальная информация о деятельности корпорации	Статья 65.2 Гражданского кодекса РФ (часть первая)

Перечень нормативных актов, относящих сведения к категории ограниченного доступа

Как передавать?

Как передавать?



Постановление Правительства Российской Федерации
от 16 апреля 2012 г. № 313

"Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)"

Как передавать?

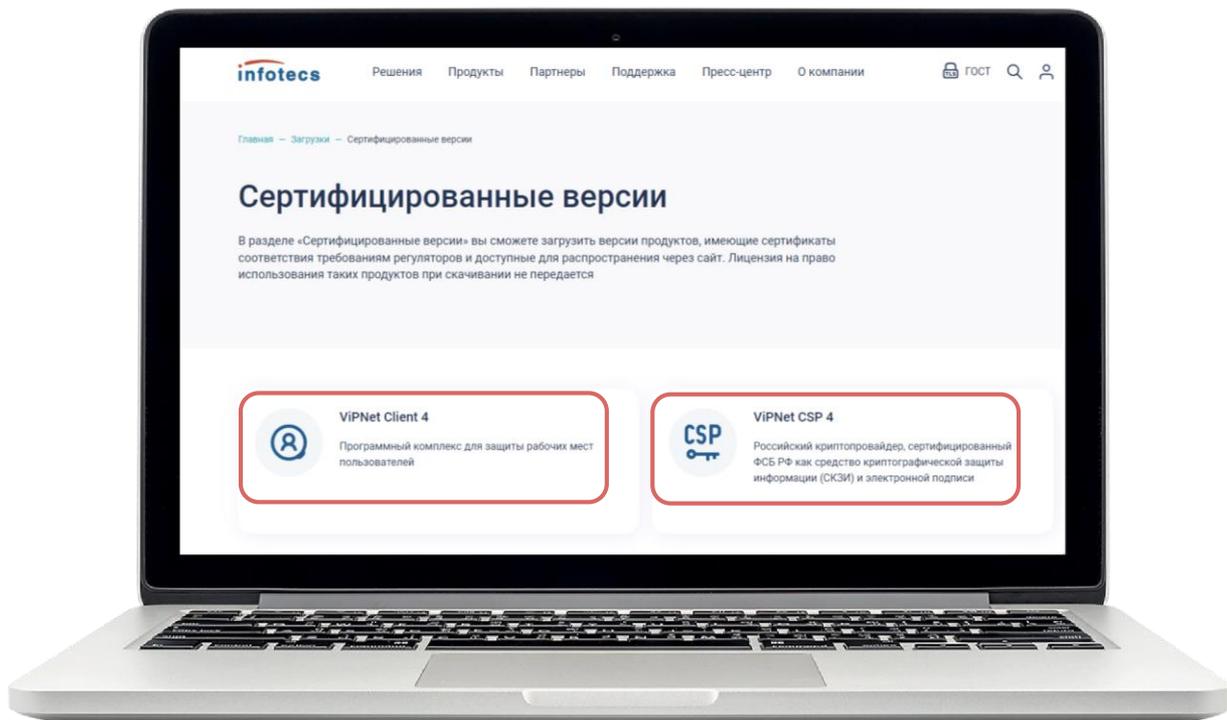


Постановление Правительства Российской Федерации
от 16 апреля 2012 г. № 313

Лицензии

- 21** Передача шифровальных (криптографических) средств <...>
- 25** Предоставление услуг по шифрованию информации <...> с использованием шифровальных (криптографических) средств <...>
- 28** Изготовление и распределение ключевых документов <...>

Скачать СКЗИ с сайта?



**А если филиал
за рубежом?**

А если филиал за рубежом?



Приложение № 9 к Решению Коллегии Евразийской экономической комиссии от 21 апреля 2015 № 30

Положение о ввозе на таможенную территорию Евразийского экономического союза и вывозе с таможенной территории Евразийского экономического союза шифровальных (криптографических) средств

ПКЗ-2005 и инструкция не регламентируют вывоз за границу



Приказ ФАПСИ от 13 июня 2001 г. № 152



2

Настоящая Инструкция не регламентирует порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации в учреждениях РФ за границей.



Положение ПКЗ-2005



5

Настоящее Положение не регулирует отношения, связанные с экспортом и импортом СКЗИ, и не распространяется на использование шифровальных (криптографических) средств иностранного производства.

Кому эксплуатировать?

Кому эксплуатировать?



Приказ ФАПСИ от 13 июня 2001 г. № 152

«Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

Требования к Администраторам

- 13 К выполнению обязанностей сотрудников органов криптографической защиты лицензиатами ФАПСИ допускаются лица, имеющие необходимый уровень квалификации для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ.
- 17 Обучение и повышение квалификации сотрудников органов криптографической защиты осуществляют организации, имеющие лицензию на ведение образовательной деятельности по соответствующим программам.
- 18 Сотрудники органа криптографической защиты должны иметь разработанные в соответствии с настоящей Инструкцией и утвержденные лицензиатом ФАПСИ функциональные обязанности.

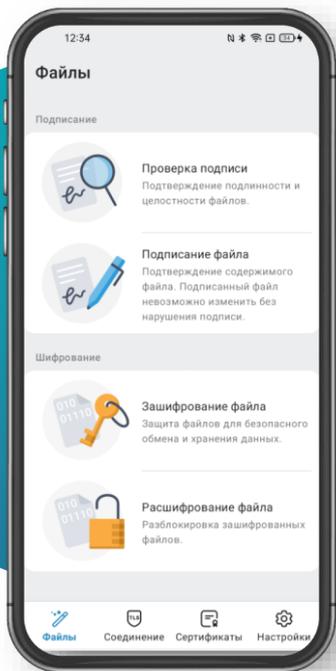
Требования к Пользователям

- 19 Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации.

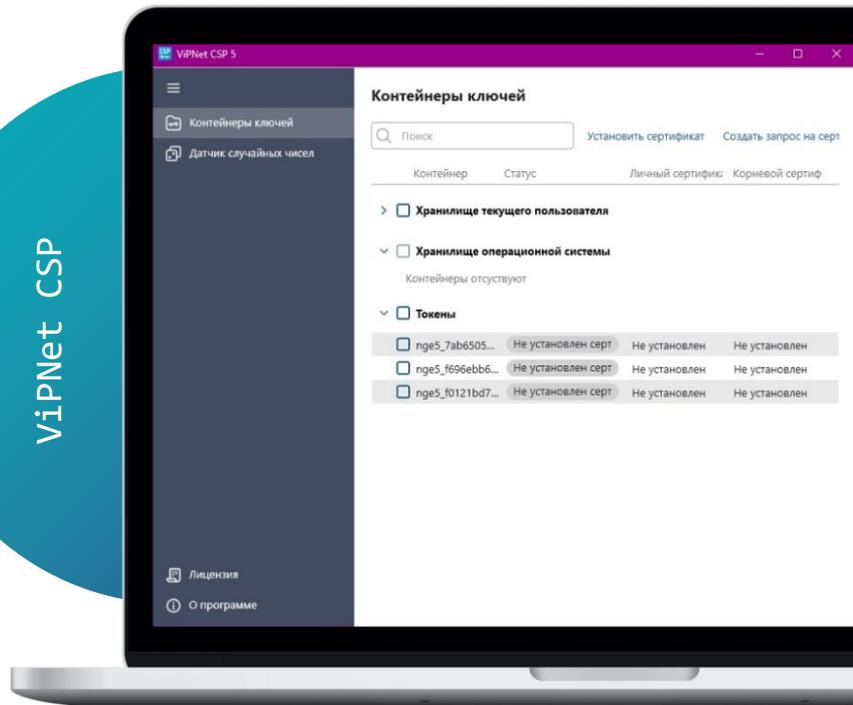
- 21 Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения. Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего органа криптографической защиты на основании принятых от этих лиц зачетов по программе обучения.

Продукты Инфотекс просты и удобны в использовании

PKI Client



VIPNet CSP



Как учитывать?

Как учитывать?



Приказ ФСБ России от 9 февраля 2005 г. № 66

«Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»



Приказ ФАПСИ от 13 июня 2001 г. № 152

«Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

Как учитывать?



Приказ ФАПСИ от 13 июня 2001 г. № 152

- 27 Все полученные обладателем конфиденциальной информации экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть **выданы под расписку** в соответствующем журнале поэкземплярного учета **пользователям СКЗИ, несущим персональную ответственность за их сохранность.**

Органы криптографической защиты заводят и ведут на каждого пользователя СКЗИ **лицевой счет**, в котором регистрируют числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы.

Типовая форма журнала учета

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		
				От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного письма	Дата и номер подтверждения или расписка в получении
1	2	3	4	5	6	7	8	9

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
Дата и номер сопроводительного письма	Дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
10	11	12	13	14	15	16

Не все так страшно



Приказ ФАПСИ от 13 июня 2001 г. № 152

29 Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) сотрудниками органа криптографической защиты под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями СКЗИ должна быть санкционирована соответствующим органом криптографической защиты.

Обладатель конфиденциальной информации с согласия органа криптографической защиты может разрешить передачу СКЗИ, документации к ним, ключевых документов между допущенными к СКЗИ лицами по актам без обязательной отметки в журнале поэкземплярного учета.

А если разрабатывается новое СКЗИ?



Правила пользования ViPNet CSP 4.4



Поэкземплярный учет СКЗИ не осуществляется в случае разработки на основе ViPNet CSP нового СКЗИ. В этом случае необходимо проводить распространение и учет СКЗИ в соответствии с документацией на разработанное СКЗИ.

Что заполнять в формуляре

- Сведения о закреплении при эксплуатации

Должность ответственного лица	Ф.И.О. ответственного лица	Номер и дата приказа		Подпись ответственного лица
		о назначении	об освобождении	

- Сведения об изменениях

Основание изменения (входящий номер сопроводительного документа и дата)	Дата проведения изменения	Содержание изменения	Порядковый номер изменения	Должность, Ф.И.О. и подпись лица, ответственного за проведение изменения	Подпись лица, ответственного за эксплуатацию продукта

**Нужна ли оценка
влияния?**

Положение ПКЗ-2005



Приказ ФСБ России от 9 февраля 2005 г. № 66

- 35 Оценка влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований осуществляется разработчиком СКЗИ совместно со специализированной организацией.
- 36 Результаты тематических исследований и оценки влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований, а также опытные образцы СКЗИ и аппаратные, программно-аппаратные и программные средства, необходимые для штатного функционирования СКЗИ, передаются в ФСБ России для проведения экспертизы.

Положение ПКЗ-2005

Приказ ФСБ России от 9 февраля 2005 г. №66 об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации

- 46 СКЗИ эксплуатируются в соответствии с правилами пользования ими. Все изменения условий использования СКЗИ, указанных в правилах пользования ими, должны согласовываться с ФСБ России и специализированной организацией, проводившей тематические исследования СКЗИ.

Формуляр на СКЗИ

На примере формуляра ViPNet CSP 4.4



При встраивании ViPNet CSP в прикладное ПО необходимо проводить (по согласованному с ФСБ России техническому заданию) оценку влияния прикладного ПО на встроенное ViPNet CSP (исполнения 1, 2, 4, 5) в следующих случаях:...

Для ViPNet CSP (исполнения 3 и 6) указанная оценка влияния проводится в обязательном порядке.

Правила пользования на СКЗИ

На примере правил пользования ViPNet CSP 4.4



Разработка прикладного ПО на основе ViPNet CSP может производиться без создания нового СКЗИ в случае использования вызовов функций из перечня, приведенного в Приложении А.

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)).

На некоторое ПО не нужна оценка влияния



Правила пользования ViPNet OSS 5.4



Для исполнений 1, 2, 4 и 5 проводить оценку влияния ПО Apache HTTP Server версии 2.4.57, Nginx версий 1.18, 1.22 и Stunnel версии 5.67 не требуется.

Зачем это все?

Приказ ФАПСИ от 13 июня 2001 г. № 152
«Об утверждении Инструкции...»

Приказ ФСБ России от 09.02.2005 № 66
«Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»

Приказ ФСБ России от 24 октября 2022 г. № 524
"Об утверждении Требований о защите информации, содержащейся в государственных информационных системах..."

Федеральный закон от 27.07.2006 № 152-ФЗ
«О персональных данных»

Указ Президента РФ от 1 мая 2022 г. № 250
«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

Приказ ФСБ России от 10 июля 2014 г. N 378
"Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных...»

Федеральный закон от 26.07.2017 № 187-ФЗ
«О безопасности критической информационной инфраструктуры Российской Федерации»

Федеральный закон от 04.05.2011 № 99-ФЗ
«О лицензировании отдельных видов деятельности»

Постановление Правительства РФ от 16.04.2012 № 313
«Об утверждении Положения о лицензировании...»

Указ Президента РФ от 30.03.2022 № 166
«О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»

Зачем это все?



СКЗИ – это еще не всё



Методические рекомендации № 149/7/2/6-432
от 31 марта 2015 г.

«Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности

(№ 149/7/2/6-432 от 31 марта 2015 г.)»

СКЗИ это еще не всё



Методические рекомендации № 149/7/2/6-432
от 31 марта 2015 г.

- 2
 - СКЗИ не предназначены для защиты информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СКЗИ не предназначены для защиты информации от раскрытия лицами, которым предоставлено право на доступ к этой информации)
 - СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ
 - СКЗИ являются как средством защиты персональных данных, так и объектом защиты

В заключение

Все это не так страшно, как кажется

- ✔ Обращайтесь к зарекомендовавшим себя вендорам
- ✔ За надежностью идите к тем, кому доверяете
- ✔ Обращайтесь в нашу лабораторию 



Пишите, если есть вопросы

Арина Эм

arina.em@infotecs.ru

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363