Всё, что вам нужно знать об оценке влияния при встраивании СКЗИ

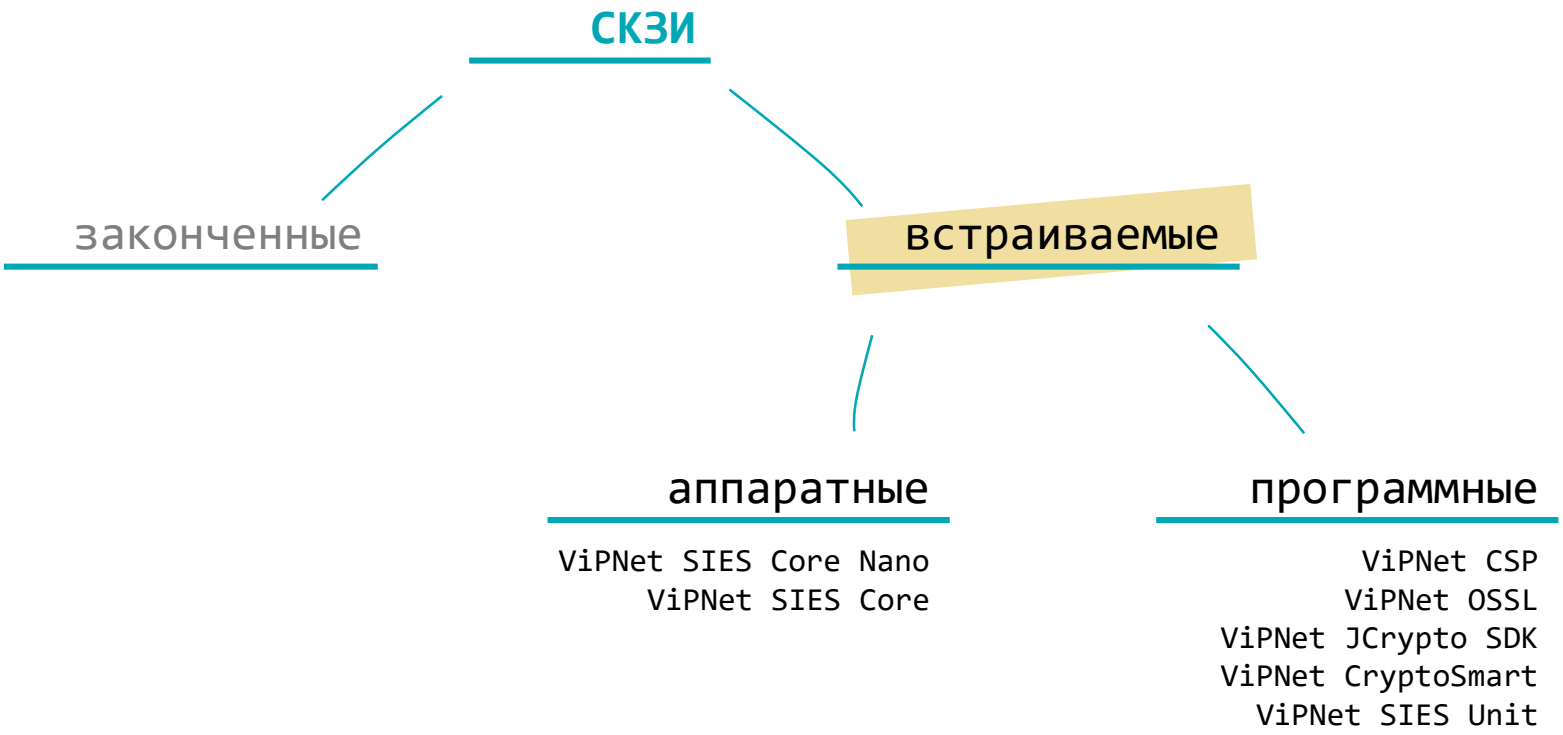
Арина Эм
Александр Бодров

infotecs

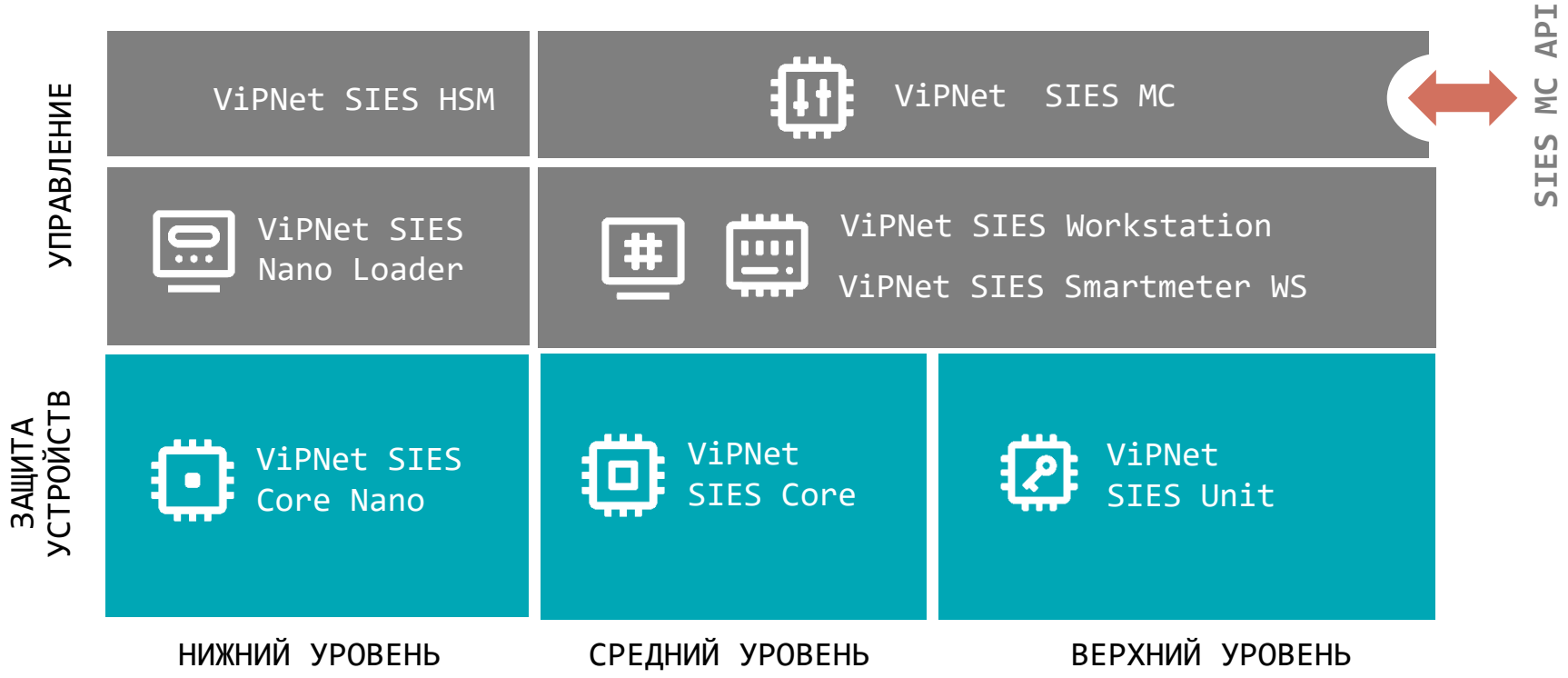
План на сегодня

1. Продукты, на которые нужна оценка влияния
2. Зачем нужна оценка влияния
3. Оценка влияния или сертификация?
4. Детали: куда обращаться и что нужно делать
5. Бонус: что, если этого не сделать
6. Ответы на вопросы
7. Розыгрыш

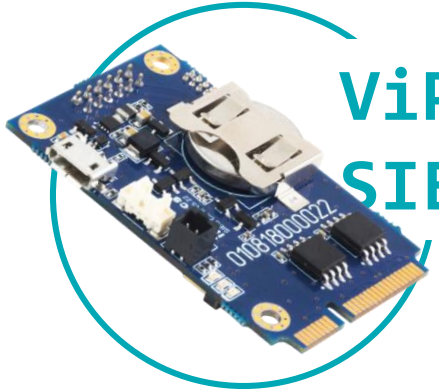
Аппаратные и программные СКЗИ



Аппаратные встраиваемые СКЗИ



Аппаратные встраиваемые СКЗИ



ViPNet SIES Core

Встраивание
- на аппаратном уровне – USB, UART, SPI
- на программном уровне – SIES Core API

Функциональные особенности
- Форм-фактор – плата PCI Express® Full-Mini Card 51 x 30 x 11,2 мм
- Возможность использования вне контролируемой зоны при использовании ДНСД
- Рабочий диапазон температур – -40…+70 ^{0}C

Сертификация
- Сертификат СКЗИ класса КС3

ViPNet SIES Core Nano

Встраивание
- На аппаратном уровне – SPI
- На программном уровне – Core Nano API

Функциональные особенности
- Форм-фактор – микросхема 3x3x0,45 мм
- Хранение ключевой информации 16 лет
- Рабочий диапазон температур -40…+85^{0}C

Сертификация
- СКЗИ-НР и СКЗИ класса КС3 (планируется на конец 2023 г.)

Программные встраиваемые СКЗИ

infotecs

ViPNet CSP

Для разработки ПО под Windows

Интерфейсы	MS CryptoAPI
Класс защиты	КС1, КС2, КС3
Сертификат ФСБ	Да

ViPNet OSSL

Для разработки мобильных и серверных решений

Интерфейсы	PKCS#11, OpenSSL
Класс защиты	КС1, КС2, КС3
Сертификат ФСБ	Да

ViPNet JCrypto SDK

Для разработки ПО на Java

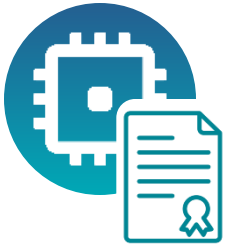
Интерфейсы	JNI/JCA, PKCS#11
Класс защиты	КС1
Сертификат ФСБ	В процессе

ViPNet CryptoSmart

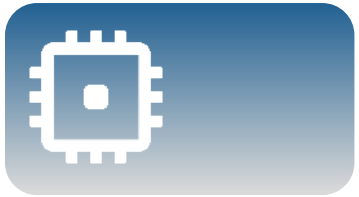
Для тех, кому нужен ГОСТ в блокчейне

Интерфейсы	MSP, NetCSP, BCCSP Lite
Класс защиты	КС1, КС2
Сертификат ФСБ	В процессе

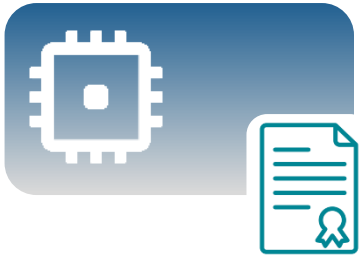
Просто встроить криптографию недостаточно



1 Найти сертифицированное СКЗИ



2 Встроить СКЗИ в ПО или ПАК



3 Провести оценку влияния

Зачем?

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

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)).

Оценка влияния или сертификация?

Что есть что?

Оценка влияния*

Вызываются функции, описанные в правилах пользования

И

само встраиваемое СКЗИ сертифицировано

Какая лицензия нужна разработчику

Лицензия на разработку защищенных с использованием шифровальных (криптографических) средств информационных систем

Создание нового СКЗИ*

Вызываются функции, **не** описанные в правилах пользования,

или

встраиваемое СКЗИ не сертифицировано

Какая лицензия нужна разработчику

Лицензия на разработку шифровальных (криптографических) средств

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

Лицензия на разработку СКЗИ имеет свои требования

Для лицензии **на разработку СКЗИ необходимо наличие** у соискателя лицензии **допуска к выполнению работ и оказанию услуг**, связанных с использованием **сведений, составляющих государственную тайну**.

Разные требования к наличию персонала (как к руководителям работ, так и к инженерно-техническим работникам).

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

Детали: куда обращаться и что нужно делать

Главные участники процесса

Испытательная лаборатория – это определенным образом аккредитованная организация, которая в лабораторных условиях проводит испытания различных видов продукции.

Органы по сертификации и испытательные лаборатории занимаются совместной работой в области сертификации.

На основании протоколов испытаний, полученных в испытательной лаборатории, орган по сертификации принимает решение о выдаче сертификата соответствия.

Для оценки влияния потребуется пакет материалов

Согласовывается с 8 Центром ФСБ России

- ТЗ на проведение оценки влияния
- Дистрибутивы ПО (СПО)
- Тест-план

Комплект документации на ПО (СПО)

- общие сведения (назначение, целевые и дополнительные функции и т.п.)
- структурная схема
- перечень собственных и сторонних библиотек и компонентов
- состав дистрибутива
- инструкция по сборке дистрибутива
- описание используемых функций СКЗИ
- перечень кодов и ошибок, получаемых при взаимодействии с СКЗИ

Определение стоимости зависит от количества сборок ИС и встраиваемых СКЗИ

Специализированная организация
проводит исследования по оценке влияния одной ИС на функционирование одного СКЗИ (общий случай)

~3 месяца

Работа завершается отправкой отчетных материалов в экспертную организацию

→

Экспертная организация
проводит экспертизу отчетных материалов по оценке влияния одной ИС на функционирование одного СКЗИ (типовая задача)

~2 месяца

По результатам экспертизы выдается заключение о соответствии требованиям

А может не надо?

Возвращаемся к ПКЗ-2005

3 Настоящим Положением необходимо руководствоваться при разработке, производстве, реализации и эксплуатации средств криптографической защиты информации конфиденциального характера в следующих случаях:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации (далее - государственные органы);
- при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд (далее - организации, выполняющие государственные заказы);
- если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;
- при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты;
- при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

Информационное сообщение ФСБ России

«О неукоснительном соблюдении операторами персональных данных требований формуляров на СКЗИ»

Обращаем внимание на обязательность неукоснительного соблюдения операторами персональных данных требований формуляров на средства криптографической защиты информации (далее – СКЗИ), в частности, **на требование, касающееся проведения оценки влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований**.

Проведение работ по оценке влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований является обязательным условием действия сертификата на СКЗИ, в соответствии с которым СКЗИ обеспечивает заданный уровень информационной безопасности при выполнении требований эксплуатационной документации согласно формуляру на СКЗИ.

<…>

Применение операторами СКЗИ, не имеющего положительного заключения ФСБ России по результатам оценки влияния аппаратных, программно-аппаратных и программных средств, если такое требование установлено в формуляре на это СКЗИ, **приводит к нарушению п. 46 Положения ПКЗ-2005 и влечет за собой административную ответственность** операторов персональных данных, предусмотренную ч. 6 ст. 13.12. Кодекса Российской Федерации об административных правонарушениях.

Все это не так страшно, как кажется

- У Инфотекс есть экспертиза и опыт
- Мы регулярно сами проводим оценку влияния для наших продуктов
- Исследовательская лаборатория СФБ Лаб в ГК Инфотекс

infotecs

Нартис успешно встроил ViPNet SIES Core в счетчики электроэнергии

НАРТИС infotecs

Мы готовы помочь

Если вы встроили наши продукты
и готовы приступить к оценке влияния,
мы предоставим шаблон ТЗ на оценку влияния!

Пишите на techpartners@infotecs.ru

Полезные ссылки

ПКЗ-2005:
Приказ ФСБ РФ от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производст... | Система ГАРАНТ (garant.ru)

152 приказ ФАПСИ
Приказ ФАПСИ от 13 июня 2001 г. N 152 "Об утверждении Инструкции об организации и обеспече... | Система ГАРАНТ (garant.ru)

Положение о лицензировании
Постановление Правительства РФ от 16.04.2012 N 313 (ред. от 03.02.2023) "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 (криптографич... - КонсультантПлюс (consultant.ru)

Информационное сообщение ФСБ России
Научно-техническая статья :: Федеральная Служба Безопасности (Научно-техническая статья) (fsb.ru)

infotecs

Спасибо за внимание

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363