КРИПТО ПРО

СКЗИ информационных технологий (СКЗИ ИТ)

Совет директоров конференции РусКрипто
Директор по научной работе ООО Крипто ПРО
Соруководитель группы сопутствующих алгоритмов ТК26 КФМН

Попов Владимир Олегович

Введение

В ноябре 2013 г. от руководства ФСБ поступило указание о пересмотре понятия СКЗИ в процессе их разработки и проведения тематических исследований. В данном документе существующая практика работы с СКЗИ определялась ключевыми словами:

– Криптоядро, встраивание, конечный продукт.

Новое представление о СКЗИ, определяемое указанием:

– функционально законченное криптосредство.

Понятие функциональной законченности в ИТ, строящихся по принципу взаимодействия открытых систем (ВОС), основывается на следующих предположениях:

– Система разбивается на функциональные блоки;
– Функциональных блок определяется интерфейсом;
– Интерфейс стандартизируется и является инвариантом блока;
– Функциональная составляющая блока поддерживает соглашения интерфейса, допустимо расширение функций блока при выполнении требований обратной функциональной совместимости.

Могут быть определены следующие подходы к понятию функционально законченного криптосредства:

– Подход ВОС;
– Подход действующих требований к СКЗИ;
– Подход нормативной базы сертификации СКЗИ;
– ПКЗ 2005;
– Существующая практика построения СКЗИ.

Место криптографии в ИТ

До недавнего времени место криптографии в ИТ определялось криптографическими услугами

- шифрования, кодами аутентификации, функциями хеширования, электронной подписи.

В последнее время в криптографической подсистеме ИТ все большее место занимают механизмы

- идентификации/аутентификации,
- авторизации.

Ключевыми понятиями, определяющими место криптографии в ИТ являются:

- пользователь ИТ,
- криптографическая подсистема ИТ,
- ИТ, обеспечивающая выполнение запросов на защищенные услуги пользователя.

Компонента криптографической подсистемы, представляемая на тематические исследования (ТИ).

Функционально законченное криптосредство.

Типизация ИТ по способу аутентификации информационных потоков

Серверные приложения.

Монопольное использование средства для обработки потока от имени администратора. (Может определять протокольный уровень криптографической подсистемы.)

Монопольное использование средства для обработки имперсонализированных данных.

- Выполняют криптографические запросы над потоками данных от имени администратора сервера с использованием потоков, имперсонализированных пользователями.
- Характеризуются широким спектром представления данных в потоке от обработки неформатированных данных до обработки протокольных данных.
- Характеризуется отсутствием оконных приложений.
- Возможно управление через удаленный терминал.

Многопользовательские приложения, АРМ пользователя.

- Выполняются запросы на криптографические услуги от имени пользователя через СРД ИТ.
- Характеризуется оконными приложениями.

Мобильные системы.

Однопользовательские системы, эксплуатируемые вне контролируемой зоны.
Характеризуются высоким уровнем интеграции криптографической подсистемы в прикладные задачи.
Характеризуются оконными приложениями.

Особенности мобильных систем:

- Проблема контроля целостности при распространения дистрибутива;
- Проблема обеспечения антивирусной защиты.

Решение данных проблем на системном уровне.

Запросы ИТ к криптографической подсистеме и запросы криптографической подсистемы к ИТ

СКЗИ в информационных технологиях должны поддерживать принципы построения информационных технологий:

- многоплатформенность и взаимодействие открытых систем;
- модульный принцип построения систем.

Кроме того, ИТ характеризуются:

- множественностью и динамичностью развития аппаратной платформы,
- множественностью и динамичностью развития ОС,
- множественностью и динамичностью развития прикладных задач,
- виртуализацией на различных уровнях,
- многозадачностью, многопоточностью.

Криптографическая подсистема определяет запросы к ИТ:

- доверие/недоверие к аппаратной платформе;
- доверие/недоверие к системному и прикладному ПО;
- высокая степень требований к защите среды выполнения криптографических запросов от нарушителей в моделях Н1 – Н3, Н5 в условиях подключения к общедоступным сетям;

Функциональная законченность криптосредства

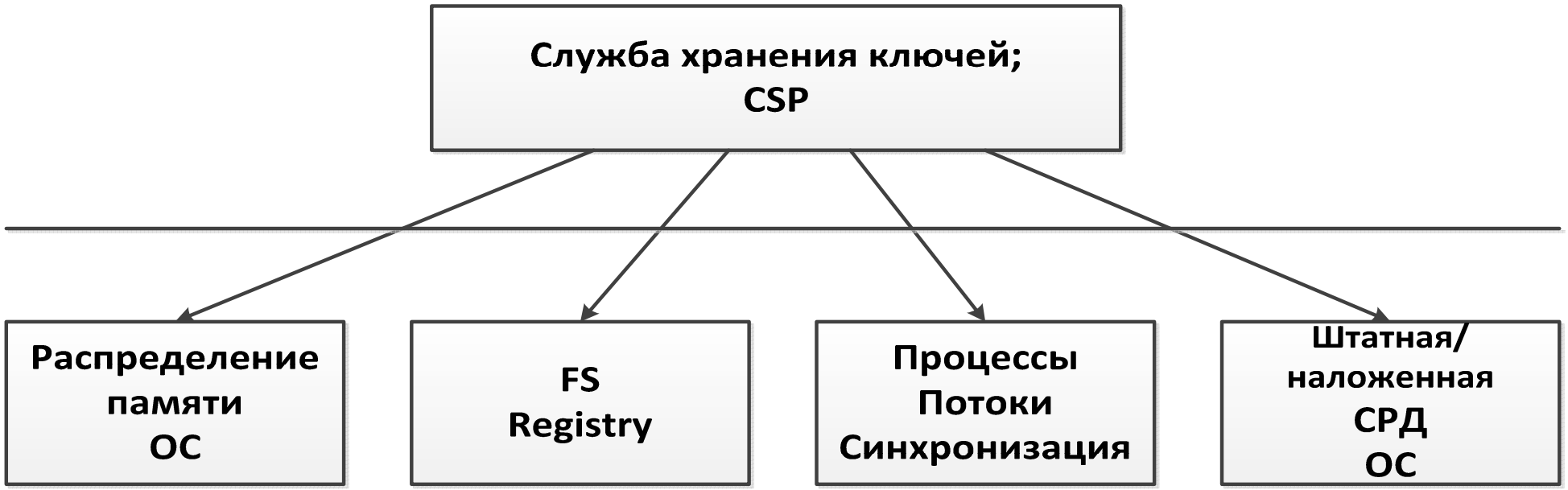
Интерфейсы криптосредства (компоненты криптосредства) разделяются на два класса:

- штатный интерфейс криптосредства представления криптографических услуг;
- интерфейс криптосредства к системному уровню ИТ (ОС) к службам распределения памяти, процессов, потоков и синхронизации, штатной системе СРД, службам runtime (время, счетчики и прочее).

Функциональную законченность криптосредства можно также трактовать как обеспечение доверия к аппаратной компоненте, системному и прикладному ПО, среде исполнения криптографических запросов.

Криптографическая законченность криптосредства (ключевая система).

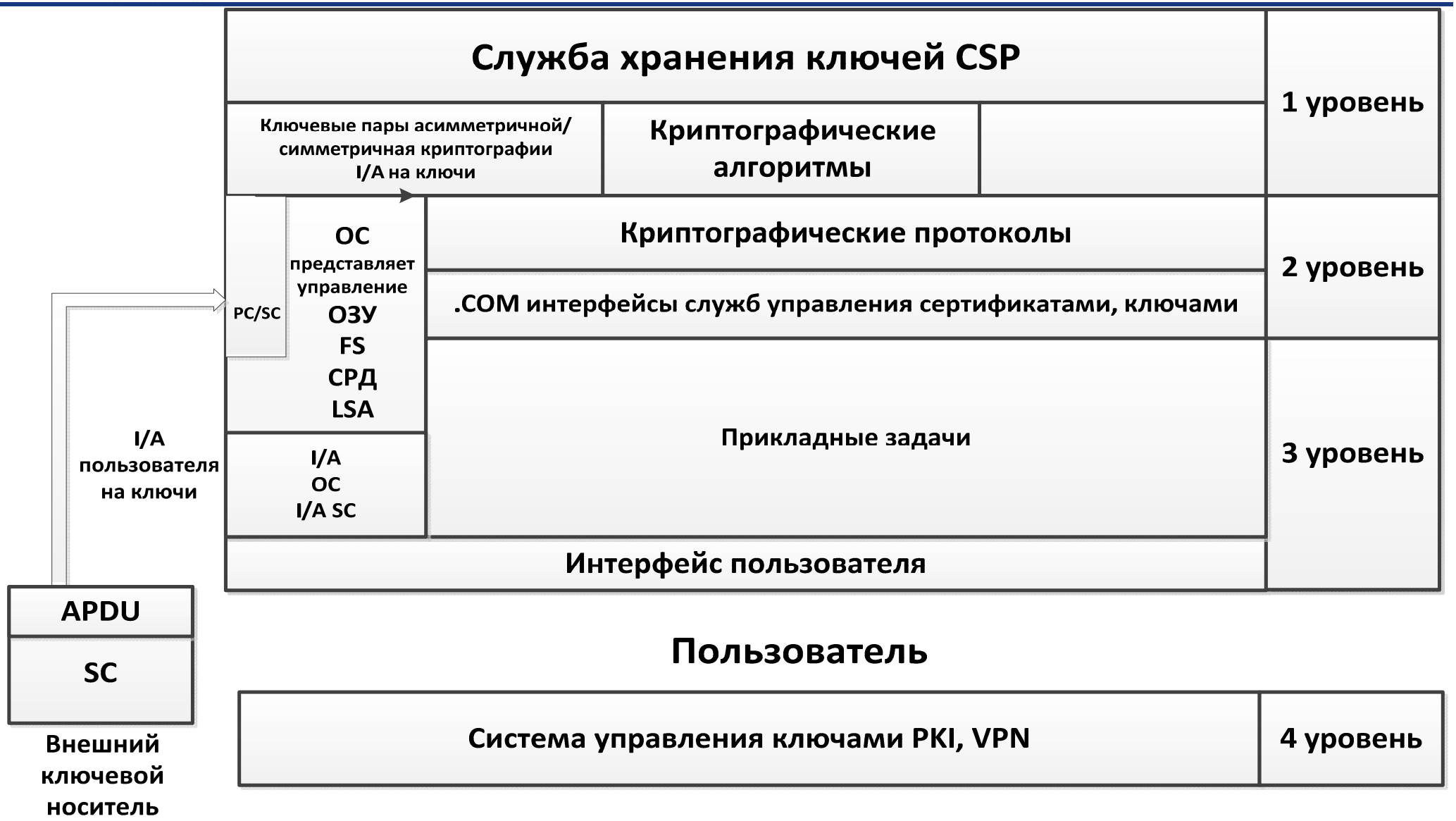
Функциональная законченность криптосредства



Службы ОС

Интересно отметить, что функциональная законченность криптосредства по отношению к системному уровню характерна для криптографической подсистемы уровня хранения ключей (1 уровень).

АРМ в Информационных технологиях



Криптографическая законченность (X.509 законченность) определяется закрытыми ключами Системы управления ключами PKI и сертификатами ключей пользователя.

Уровни криптографической подсистемы ИТ

Сложившаяся практика использования криптографических подсистем позволяет выделить 4 уровня:

1. Уровень хранения ключей (ключевые пары, ключи и неструктурированные данные, механизмы шифрования, MAC, хеширование, ЭЦП), (CSP).

2. Уровень криптографических протоколов (токены доступа, сертификаты, протокольные сообщения), (CSP + сертификаты, revocation provider).

3. Уровень защищенных услуг ИТ пользователя (субъекты доступа и информация субъекта доступа).

4. Уровень распределения ключей (субъекты доступа и ключи субъекта доступа).

Уровни криптографической подсистемы характеризуются:
- функционалом (механизмами) и объектами;
- интерфейсами и SDK.

Уровень хранения ключей (уровень 1)

Данный уровень определяет хранения открытых/закрытых симметричных ключей пользователя, выполнение криптографических функций стандартов защиты данных и сопутствующих алгоритмов.

Функциональный набор данного уровня является достаточным для проведения операций с ключевой информацией.

Определяет собственную систему аутентификации/идентификации на ключи пользователя.

От СРД операционной системы наследует процессы пользователя, security идентификаторы пользователя.

Представляется интерфейсами: CryptoAPI 1.0 (CSP), CNG, PKCS#11 и иные.

Функционально определяется стандартами криптографической защиты данных и сопутствующими алгоритмами, определенными в документации Р 34.10, Р 34.11, 12847-89, RFC 4357, методическими рекомендациями ТК26 (сопутствующие алгоритмы, параметры стандартов, режимы шифрования).

Интерфейсная часть определяется в SDK, соответствующие модули выполняются в CSP.

Состав механизмов, связанных с обработкой ключевой информации, подсистемы хранения ключей достаточен для выполнения запросов криптографической подсистемы протокольного уровня.
Законченность данного уровня – обеспечение безопасного использования ключей в ИТ.

Требует надстройки системы управления и контроля сертификатов для обеспечения функциональной законченности в криптографическом смысле.

Уровень криптографических протоколов (уровень 2)

Определяет криптографические протоколы и службы:

- CAPI 2.0, NSS
- CMS
- TLS, IPSec, EFS, LogOn, Kerberos…
- CA, TSP, OCSP, Cades,…

Выполняется в процессах пользователя, либо в имперсонализированных потоках пользователя.

Выполняет криптографические запросы от имени пользователя на основе токенов доступа.

Характеризуется интерфейсами:
CryptoAPI 2.0, SSPI, .COM, NSS, EMV, и др.
Определяется документами ТК 26: методические рекомендации, технические спецификации X.509, CMS, TLS, IKE v.1, ESP, AH.

Законченность данного уровня – обеспечение идентификации/аутентификации, авторизации криптографических услуг в среде ИТ.

Уровень представления защищенных услуг ИТ пользователю (уровень 3)

Определяет уровень представления защищенных информационных услуг пользователю.

Определяет систему идентификации/аутентификации пользователя к ИТ.

Определяет способы управления ключами пользователя при обращении к ИТ.

Выполняет услуги защищенной почты, браузера, защиты локальных ресурсов.

Представляет интерфейсы пользователя.
Обеспечивает связь пользователя с СРД операционной системы.
Разделяет интерфейс к функциям криптографической подсистемы в части управления ресурсами подсистемы.

Законченность данного уровня – представление криптографических услуг пользователю ИТ.

Стеки интерфейсов (криптографических средств), протоколов подсистемы уровня представления защищенных услуг.

Защищенная услуга	Крипт. подсистема уровня 1	Крипт. подсистема уровня 2	Крипт. подсистема уровня 3	Комментарий
Почта	CAPI 1.0	CAPI 2.0	OUTLOOK	
Защищенная файловая система (EFS)	CAPI 1.0	CAPI 2.0	LSA. LOGON. …	Прикладной уровень
	CAPI 1.0	CAPI 2.0	FS. LSA. LOGON. … FS. …	Прикладной уровень Уровень ядра ОС
Защита IP (IPSec)	CAPI 1.0	CAPI 2.0. IKE	UDP LSA. LOGON. …	Сетевой уровень Прикладной уровень
	CAPI 1.0	ESP	IP. …	Уровень ядра ОС
Защита браузера (TLS)	CAPI 1.0	CAPI 2.0. SSPI	LSA. LOGON. …	Прикладной уровень Приложения Windows
	PKCS#11	NSS.TLS (и процесс LSB)	FireFox ThanderBird	Уровень ядра Приложения Unix
Электронная подпись (генерация)	CAPI 1.0	… Cades	… (Использование в монопольных системах)	В зависимости от уровня запросов ИТ
Электронная подпись (проверка)	CAPI 1.0	CAPI 2.0. TSP. OCSP	LSA. LOGON. …	

Уровень распределения ключей (уровень 4)

Обеспечивает выполнение запросов пользователя по управлению ключами ключевой системы (симметричная, асимметричная криптография).

В случае асимметричной криптографии реализуется службами PKI:

- CA
- ЦР
- TSP
- OCSP
- АРМ пользователя

На данном уровне обеспечивается криптографическая законченность ИТ.

Выводы

1. С точки зрения пользователя функционально законченным криптосредством является криптосредство уровня 3-4 ИТ, обеспечивающий полный комплекс криптографических услуг.
2. С точки зрения ИТ функционально законченным криптосредством может быть определено криптосредство уровня 1 или уровня 2, в зависимости от спектра запросов, определяемых данной технологией.
3. С точки зрения криптографической подсистемы функционально законченными криптосредствами могут быть определены:
    - Служба хранения ключей (уровень 1)
    - Служба криптографических протоколов (уровень 2)
    - Служба предоставления защищенных услуг пользователю (уровень 3)
    - Служба управления ключами (уровень 4)

1. Все перечисленные службы включаются в ИТ через интерфейсы, определяемые SDK.
2. Практика использования интерфейсов показывает, что криптографически безопасных интерфейсов не существует.
3. Все криптографические интерфейсы потенциально опасны в ИТ. Все они требуют контроля корректности использования в ИТ.

Вопросы

ВОПРОС: Допустимо ли использование только аппаратных СКЗИ?

ОТВЕТ: В условиях приоритетного использования механизмов идентификации/аутентификации, авторизации вся ИТ пронизывается криптографическими средствами.

Дальнейшие темы:
- Нормативная база СКЗИ и классификация СКЗИ ИТ.
- Вопросы тематических исследований и сертификации СКЗИ и классификация СКЗИ ИТ.

КРИПТО ПРО

СПАСИБО ЗА ВНИМАНИЕ!

http://www.cryptopro.ru
vpopov@cryptopro.ru

Тел./факс:
+7 (495) 780-48-20
+7 (495) 660-23-30