Концепция СКЗИ информационных технологий

Тезисы выступления на конференции РусКрипто 2014
Попов В.О.
Совет директоров конференции РусКрипто.
Директор по научной работе ООО Крипто ПРО.
Соруководитель группы сопутствующих алгоритмов ТК26.

Введение

В ноябре 2013г. 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, 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

Из рассматриваемых подходов только подход ВОС связан с функциональной законченностью криптосредств, в связи с чем задача определения понятия функциональной законченности криптосредства актуальна и рассматривается в данной концепции.

До недавнего времени место криптографии в ИТ определялось криптографическими услугами

- шифрования,
- коды аутентификации,
- функции хэширования,
- электронная подпись.

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

- идентификации/аутентификации,

- авторизации.

Это, в свою очередь, приводит к принципиальному пересмотру взаимодействия криптографической подсистемы и системы разграничения доступа (СРД) штатной операционной системы, наложенной СРД. Если раньше криптографические услуги представлялись СРД для решения задач разграничения доступа, то теперь криптография, обеспечивая идентификацию/аутентификацию и авторизацию, определяет участие пользователя в подсистеме, передает СРД идентификаторы/аутентификационные элементы пользователя, которые, в свою очередь, обеспечивают выполнение криптографических услуг от имени пользователя.

Данное отношение к криптографическим средствам особенно было подчеркнуто принятием ФЗ «Об электронной подписи».

1. Место криптографии в ИТ

Ключевыми понятиями, определяющими место криптографии в ИТ являются:

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

Основные элементы и функции данных компонентов.

Пользователь ИТ:

- Определяет требования по защищенным услугам к ИТ;
- Проводит процедуру идентификации и аутентификации;
- Представляет ИТ ключи и сертификаты;
- Использует в операциях интерфейс пользователя к системе ИТ.

Информационные технологии:

- Адаптирует информацию идентификации/аутентификации и создает объект «токен доступа»;
- Запускает процессы от имени пользователя или персонализирует процессы ИТ от имени пользователя на основе токена доступа;
- Создает криптографические запросы от имени пользователя к криптографической подсистеме;

Криптографическая подсистема:

- Используется для функций идентификации/аутентификации пользователя и обеспечивает криптографическую валидность токена доступа;
- Обеспечивает выполнение криптографических запросов от имени пользователя на основе принципов разграничения доступа, включающих
    - Функционирование криптографической подсистемы в составе процесса пользователя;
    - Функционирование криптографической подсистемы в составе сервиса потоком, имперсонализированным от имени пользователя;
    - Выполнение криптографических запросов от имени пользователя, контролируемых токеном доступа

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

Определяется соглашением сторон о достаточности состава компоненты с точки зрения выполнения криптографических требований.

Функциональная законченность криптосредства:

Определяется системой интерфейсов компонента криптографической подсистемы.

Таким образом, в системе взаимодействия ИТ и криптографической подсистемы должны выполняться требования по доказуемости выполнения криптографических запросов от имени пользователя за счет передачи токенов доступа через среду СРД ИТ и через систему процессов, запущенных от имени пользователя, либо потоков, имперсонализированных от имени пользователя.

2. Типизация ИТ по способу аутентификации информационных потоков

2.1 Серверные приложения.

Монопольное использование средства для обработки потока от имени администратора.

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.

2.2 Многопользовательские приложения, АРМ пользователя.

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

2.3 Мобильные системы.

Однопользовательские системы, эксплуатируемые вне контролируемой зоны.

Характеризуются высоким уровнем интеграции криптографической подсистемы в прикладные задачи.

Характеризуются оконными приложениями.

Особенности мобильных систем:

- Широкое распространение APPStory и систем контроля распределения дистрибутива на основе криптографии RSA.
- Антивирусная защита приложений имеет ограниченное значение, в частности, iOS, связанное с изоляцией приложения в среде исполнения при условии невзломанности системы.

3. 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;

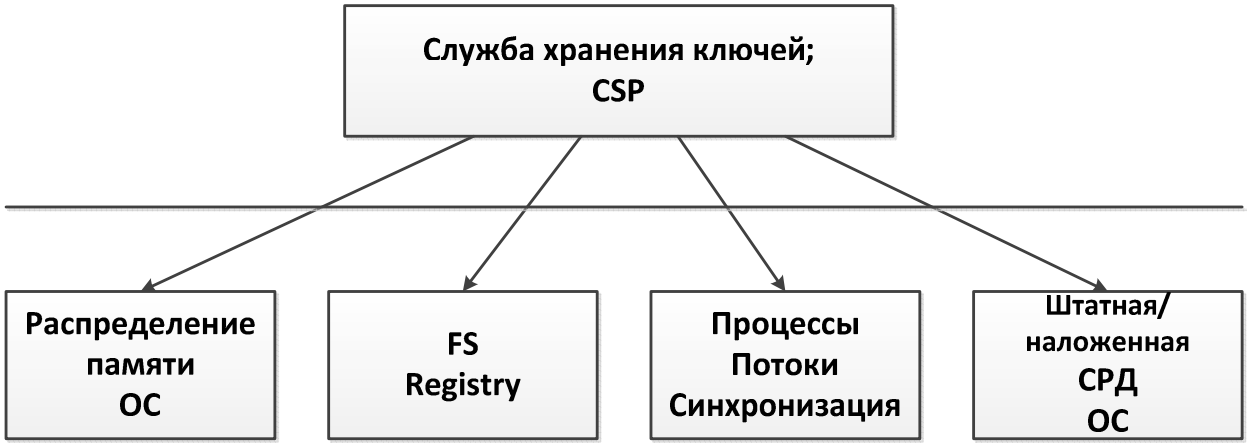
4. Функциональная законченность криптосредства

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).



Службы ОС

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

1. АРМ в Информационных технологиях

АРМ Пользователя

Криптографическая законченность (X.509 законченность) определяется закрытыми ключами Системы управления ключами PKI, в частности ключом корневого УЦ, и сертификатами ключей пользователя, в частности корневым сертификатом при условии доверенного распределения и хранения корневого сертификата.

2. Уровни криптографической подсистемы ИТ

Сложившаяся практика использования криптографических подсистем позволяет выделить 4 уровня:
Уровень хранения ключей
Уровень криптографических протоколов
Уровень защищенных услуг ИТ пользователя
Уровень распределения ключей

2.1 Уровень хранения ключей (уровень 1)

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

Как правило, 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.

Представляет низкоуровневые криптографические услуги для выполнения криптографических протоколов и служб.

Представляется интерфейсами:
CryptoAPI 1.0 (CSP)
PKCS#11
CNG

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 в форме инсталлятора, определяющего установку системных dll, либо в форме сервиса, включающего данный совокупность dll.

2.2 Уровень криптографических протоколов (уровень 2)

Определяет криптографические протоколы и службы:

TLS, IPSec, EFS, CMS,…
CA, TSP, OCSP, Cades,…

Выполняется в процессах пользователя, либо в имперсонализированных нитях 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.

2.3 Уровень защищенных услуг ИТ пользователя (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.

Стеки интерфейсов, 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	–	File System	Уровень ядра ОС
Защита IP (IPSec)	CAPI 1.0	CAPI 2.0. IKE	UDP LSA. LOGON. …	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	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. …	

2.4 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

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