ВОПРОСЫ РЕАЛИЗАЦИИ ПРОТОКОЛОВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ. РОССИЙСКИЕ ГОСТ-Ы И IPSEC, TLS, EFS, ФКН

В.Попов

ООО Крипто Про

Что должна защищать криптография - требования

- **Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных" от 21 февраля 2008 года (www.zki.infosec.ru/law/personal/)**

- **I. Общие положения**

- **2. Организация и обеспечение безопасности обработки персональных данных с использованием шифровальных (криптографических) средств.**

- **3. Порядок обращения с криптосредствами и криптоключами к ним. Мероприятия при компрометации криптоключей.**

- **4. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним.**

Что должна защищать криптография - требования

- **Типовые требования …**

- 2.3. При разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в информационной системе оператор или уполномоченное оператором лицо осуществляет:
- ***- разработку для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;***
- ***- разработку на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;***
- - определение необходимости использования криптосредств для обеспечения безопасности персональных данных …;
- - установку и ввод в эксплуатацию криптосредств …;
- - проверку готовности криптосредств к использованию …;
- - поэкземплярный учет используемых криптосредств, …;
- - учет лиц, допущенных к работе с криптосредствами,…;
- - контроль за соблюдением условий использования криптосредств, …;
- - разбирательство и составление заключений по фактам нарушения условий хранения носителей персональных данных, использования криптосредств, …;
- - описание организационных и технических мер …

Что должна защищать криптография - методология

- **Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации" от 21 февраля 2008 года (www.zki.infosec.ru/law/personal/)**

- **2. Основные положения**
- **3. Методология формирования модели угроз**
- ***Методология формирования детализированной модели угроз***
- ***Методология формирования модели нарушителя***
- шесть основных типов нарушителей: H_1, H_2, ... , H_6.
- ***Предположения об имеющейся у нарушителя информации об объектах атак, средствах атак, описание каналов атак.***
- **4. Уровень криптографической защиты персональных данных, уровни специальной защиты от утечки по каналам побочных излучений и наводок и уровни защиты от несанкционированного доступа.**
- шесть уровней КС1, КС2, КС3, КВ1, КВ2, КА1 криптографической защиты

Что должна защищать криптография - методология

- **Методические рекомендации …**

- 2.2. В соответствии с п. 2 Положения (ПКЗ-2005) безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, ***включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.*** Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

- ***Описание информации, сопутствующей процессам создания и использования персональных данных***
- На основе анализа условий создания и использования персональных данных должна быть определена информация, сопутствующая процессам создания и использования персональных данных. При этом представляет интерес только та информация, которая может быть объектом угроз и потребует защиты.
- **К указанной информации, в частности, относится:**
- **- ключевая, аутентифицирующая и парольная информация криптосредства;**
- **- криптографически опасная информация (КОИ);**
- **- конфигурационная информация;**
- **- управляющая информация;**
- **- информация в электронных журналах регистрации;**
- **- побочные сигналы, которые возникают в процессе функционирования технических средств и в которых полностью или частично отражаются персональные данные или другая защищаемая информация;**
- - резервные копии файлов с защищаемой информацией, которые могут создаваться в процессе обработки этих файлов;
- **- остаточная информация на носителях информации.**

Стандарты и протоколы криптографической защиты информации

- *Стандарт шифрования и имитозащиты: ГОСТ 28147 89г.*
- *Процессы формирования и проверки электронной цифровой подписи: ГОСТ Р 34-10 2001г.*
- *Функция хеширования: ГОСТ Р 34-11 89г.*
- - СКЗИ и системный подход к защите информации; вопросы взаимодействия систем различного уровня защищённости;
- - СКЗИ и криптографические протоколы:
- - уровень преобразования ключей в ключевых системах RFC 4357
- - уровень организации транспорта ключей и ЭЦП (CMS) RFC 4490, RFC 4491
- - крптографические протоколы:
- TLS проект RFC,
- IPSec проект RFC протоколов IKE, ESP, AH,
- EFS продукт,
- ФКН (защита персональных ключей пользователя на смарткартах);
- - удостоверяющий центр и службы УЦ (tsp, ocsp)
- - КрипоАРМ
- - HSM, клиент HSM

2. Организация и обеспечение безопасности обработки с использованием шифровальных (криптографических) средств персональных данных

- Пользователи криптосредств
  - АРМ пользователя
    - Цели и задачи: обеспечение документооборота конечного пользователя в условиях выполнения требований по защите информации конечного пользователя
- Операторы криптосредств
  - АРМ оператора
    - Цели и задачи: обеспечение управления безопасностью сети документооборота в условиях выполнения требований по защите системы документооборота
- Администраторы безопасности
  - Сервера системы документооборота (сервер доступа, сервер базы данных и т.п.)
    - Цели и задачи: обеспечение безопасности элементов массового доступа в системе документооборота в условиях выполнения требований по защите системы документооборота

Определение АРМ пользователя, АРМ оператора, сервера

- По целевой функции – перечень прикладных задач документооборота
- По способу подключения к сети
  - Изолированный
  - Локальная сеть
  - Корпоративная сеть
  - VPN
  - Глобальная сеть
- По системе защиты
  - Модель нарушителя и уровень защищённости
  - Модель защиты АРМ′а, СРД
  - Криптографическая подсистема и система криптографических протоколов
  - Система криптографических ключей
- Аппаратная составляющая АРМ
- Программная составляющая АРМ
  - ОС
  - Прикладное программное обеспечение
- По требованиям доступности АРМ пользователям, операторам, администраторам безопасности.
  - Персональные
  - Общего использования

Таблица уровней защиты АРМ

	Тип подключения	Модель нарушителя	Уровень безопасности
АРМ Пользователя	Изолированный	Н1 – Н3	КС1 – КС3, КВ1 – КВ2
	Локальная сеть	Н1 – Н3	КС1 – КС3
	Корпоративная сеть	Н1 – Н3	КС1 – КС3
	VPN	Н1 – Н5	КС1 – КС3, КВ1 – КВ2
	Глобальная сеть	Н1 – Н5	КС1 – КС2
АРМ Оператора	Изолированный	Н1 – Н5	КС1 – КС3, КВ1 – КВ2
	Локальная сеть	Н1 – Н3	КС1 – КС3
	Корпоративная сеть	Н1 – Н3	КС1 – КС3
	VPN	Н1 – Н5	КС1 – КС3, КВ1 – КВ2
	Глобальная сеть	Н1 – Н5	КС1 – КС2
Сервер	Изолированный	Н1 – Н3	КС1 – КС3, КВ1 – КВ2
	Локальная сеть	Н1 – Н3	КС1 – КС3
	Корпоративная сеть	Н1 – Н3	КС1 – КС3
	VPN	Н1 – Н5	КС1 – КС3, КВ1 – КВ2
	Глобальная сеть	Н1 – Н5	КС1 – КС2

Необходимость сетевого взаимодействия устройств разного уровня защищённости

Средства защиты АРМ в условиях использования СКЗИ

Уровень защиты	Гарантии доступа к АРМ	Разграничение доступа	Антивирусная защита	Контроль среды	Защита сетевого доступа	Защита данных в АРМ	Гарантии ОС и ППО	Гарантии на аппаратуру
КС1	Штатные средства ОС	Штатные средства ОС	Требуется АВ защита	Штатные средства ОС	Орг. Тех. меры	Орг. Тех. меры	Лицензионные, фиксир. набор	Общего назначения
КС2	Аппаратные средства	----#----	----#----	----#----	----#----	----#----	----#----	----#----
КС3	----#----	Верифицированные СРД	----#----	Верифицированные средства	Криптографическими мерами	Криптографическими мерами	----#----	----#----
КВ1 – КВ2	Доверенная загрузка	----#----	----#----	Изолированная среда	----#----	----#----	Гарантированные ОС и ППО	Спецтального назначения

Задача организации взаимодействия АРМ пользователя, защищённого по низким уровням (КС1) с серверами доступа, защищёнными по высоким уровням (КВ2).

EFS

- 1. Определение Крипто Про EFS.
- 2. Шифрование и имитозащита с использованием irp.
- Ключ вырабатывается по схеме
- $K_П = KeyTree(K, n, irp)$
- , где n – смещение.
- $$KeyTree \ :$$
  $$K_1 = Divers\ (K, n \ \& \ c_1)$$
  $$K_2 = Divers\ (K, n \ \& \ c_2)$$
  $$K_3 = Divers\ (K, n \ \& \ c_3)$$
  $$K_П = Divers\ (K, \text{irp})$$
- Обеспечивается защита ключей от повтора при зашифровании (irp – случайная величина, вырабатывается FS при записи очередной последовательности данных (секторов)).
- 3. Запись irp, Imit в отдельный поток файла (в самостоятельные секторы файла).

Схемы встраивания СКЗИ в криптографические протоколы

1. Защита соединения, интерфейс SSPI

   Ключевые понятия: credential

   - идентификаторы пользователя.
   - SID.
   - Права и привилегии.

   Пример: КриптоПро TLS.

2. На уровне криптографических вызовов интерфейса СКЗИ.
3. На уровне защиты пакета.

   Пример: интерфейс модулей КриптоПро IPSec.

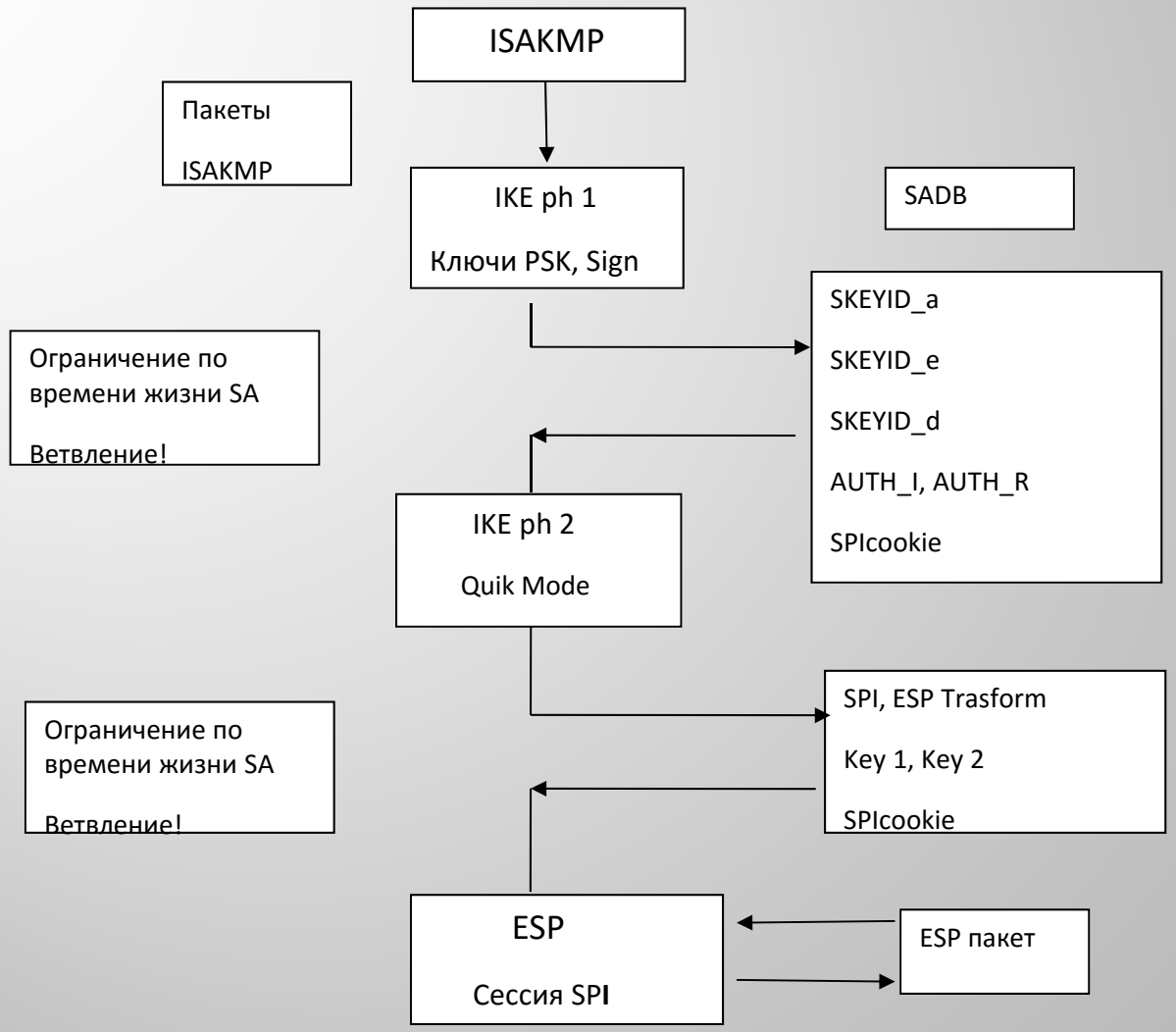
Процедура сертификации криптографического протокола и криптосредства.

Пример: в случае IPSec в состав криптосредства включается сетевая компонента OS.

TLS

- 1. Аутентификация на статических ключах Diffie-Hellman либо на ключе ЭЦП.
- 2. Защита потока шифрованием в режиме CRYPT_PROMIX_MODE (со сменой ключа через 1К).
- 3. Использование имитозащиты с зацеплением блоков.

Структура IPSec



Структура ESP

- На входе: SPI, K_1, SPI_cookie.
- Управление ключами: $K_П = KeyTree(K, Sec\#)$

$$KeyTree \ :$$
$$K_1 = Divers\ (K, Sec\ \#\&\ c_1)$$
$$K_2 = Divers\ (K, Sec\ \#\&\ c_2)$$
$$K_П = Divers\ (K, Sec\ \#\&\ c_3)$$

- В составе пакета: SPI, [Seq#] (low), IV_Random, IV_Counter.

IV_Counter=SPI_Cookie+SPI+[Seq#] (low) +IV_Random.

Перечень отличий и мотивация

1. Шифрование и сквозная имитозащита пакетов ISAKMP в отличие от шифрования RFC 2409.
2. Введены Message_Nonce наряду с Message_ID.
3. Передача в Фазу 2 дополнительной величины SPI_Cookie, AUTH.
4. Вычисление IV фазы 2:

   IV=substr(0..7,

   Hash(Last_ICV,Message_ID,Message_Nonce).
5. SK_a=PRF(SKEYID_a, Message_ID, Message_Nonce, A_I, A_R);

   SK_e=PRF(SKEYID_e, Message_ID, Message_Nonce, A_I, A_R).
6. Дерево ключей ESP, AH.
7. Использование SPI_cookie в IV пакета.

ФКН

Протокол EKE, Q_{PW} - точка элептической кривой строится по паролю, задача: сложность определения пароля по данным протокола.

	ФКН	**CSP**
0	Q_{PW} , id_x	Q_{PW} , id_x , x
1		1. $rndm$ α , $Q_\alpha = e[id\_x]\alpha P$; 2. $u_1 = Q_\alpha + Q_{PW}$;
2		$\Leftarrow$ u_1
3	1. Проверка: $u_1 \in G$? 2. $Q_\alpha = u_1 - Q_{PW}$; 3. $rndm$ β ; 4. $Q_\beta = e[id\_x]\beta P$; 5. $u_2 = Q_\beta + Q_{PW}$	
4	u_2 $\Rightarrow$	
5		1. $u_3 = x + \alpha(u_2 - Q_{PW})$, если x - точка, 1'. $u_3 = x \oplus x_{\alpha(u_2 - Q_{PW})}$, если x - число или бинарный массив
6		$\Leftarrow$ u_3
7	1. $K_{EKE} = \beta Q_\alpha$; 2. $data = u_3 - K_{EKE}$, если x - точка, $data = u_3 \oplus x_{K_{EKE}}$, если x - число или бинарный массив; 3. Если $id \neq id\_x$, то dec c_4 , dec c_5 ; 4. dec c_1 ; 5. если $c_1c_2c_3c_4c_5 = 0$ - **ERROR,** иначе 6; 6. $x = data$	

Потенциальные атаки на ключи в вычислительной системе (ФКН)

- перехват ключевого контейнера при считывании с носителя в ВС и записи его из ВС на носитель;
- перехват пароля при вводе его в ВС;
- перехват ключевого контейнера и пароля (выработанного из пароля ключа) при их хранении в ВС;
- перехват ключа в памяти ВС;
- перехват из памяти ВС информации о ключе при выполнении операций с ключом;
- несанкционированное использования ключа и криптографического функционала.

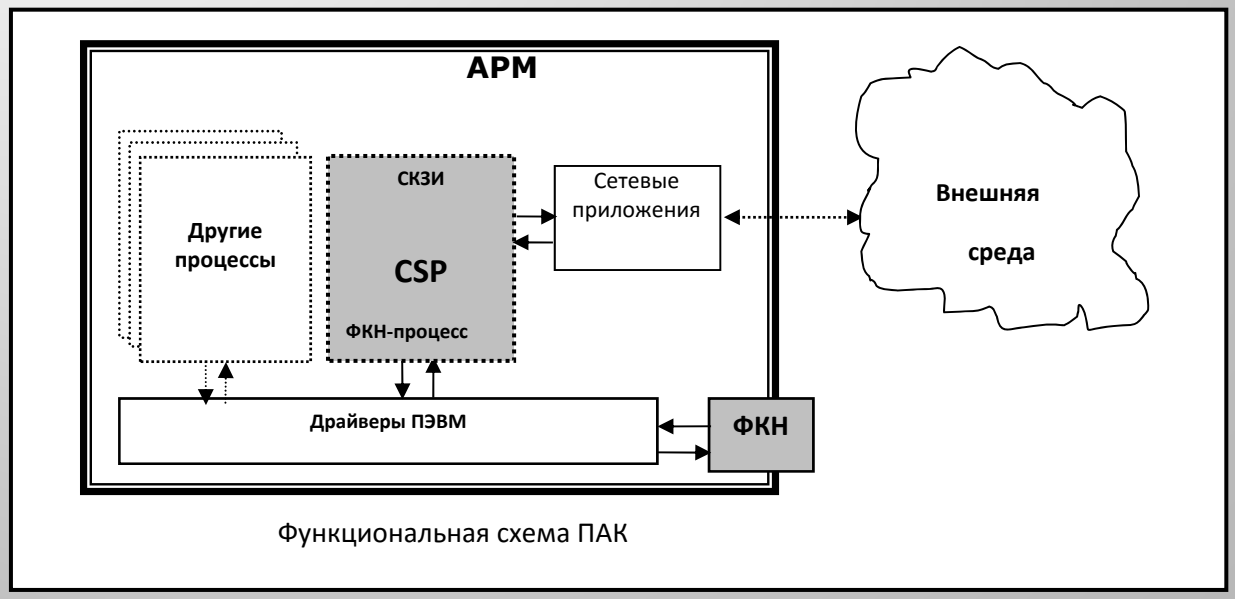
Функциональный ключевой носитель (ФКН) на смарткарте

С использованием ФКН на смарткарте (SC) связаны следующие возможности:

- доступ к работе с SC только по предъявлении пароля (pin-кода);
- генерация, хранение, использование и уничтожение (вывод из действия) ключей в SC;
- опциональная возможность доступа к ключу в SC по предъявлении пароля на ключ;
- защита ключа от экспорта из SC штатными средствами SC;
- выполнение в SC криптографических функций (формирование ЭЦП, вычисление ключа Диффи-Хеллмана).
- экспорт из SC только результатов выполнения криптографических функций.

Актуальность разработки системы ФКН. Проблема доверия к системе SC – BC

Функционал	Уровень доверия к SC	Уровень доверия к BC
Генерация ключей	Нет доверия к ДСЧ	Доверяем ДСЧ
Хранение ключей	Доверяем	Нет доверия
Криптографический функционал	Требует обоснования	Доверяем



Функциональная схема ПАК

Протокол парольной аутентификации на ключ в системе SC– BC на базе протокола EKE, [1, п. 22.5].

Протокол EKEinCS передачи параметра x из BC в SC

	SC	BC
	Начальное состояние: Q_{pw}, id_x,	Начальное состояние: Q_{pw}, id_x, x ,
1		rndm a, $Q_a = e[id\_x]aP$; $u1 = Q_a + Q_{pw}$;
2		$\Leftarrow u1$
3	$Q_a = u1 - Q_{pw}$; rndm b; $Q_b = e[id\_x]aP$; $u2 = Q_b + Q_{pw}$;	
4	$u2\Rightarrow$	
5		$Q_b = u2 - Q_{pw}$; $K_{EKE} = aQ_b$; $u3 = K_{EKE} + x$,
6		$\Leftarrow u3$
7	$K_{EKE} = bQ_a$; data = $u3 - K_{EKE}$	
8	Двусторонняя аутентификация на базе ключа K_{EKE}	Двусторонняя аутентификация на базе кюча K_{EKE}

Q_{pw}- ключ аутентификации SC с BC, вырабатываемый при инсталляции системы SC – BC из пароля пользователя, должен доставляться в карту по защищённому каналу, вопросам обоснования выбора значения Q_{pw} и стойкости протокола EKE на паролях посвящено много работ, см., в частности, [2]

- Аналогично строится протокол EKEoutCS.
- Протокол EKE: Q_{pw} - точка эллептической кривой строится по паролю, задача: сложность определения пароля по данным протокола.