Программно-аппаратные средства обеспечения информационной безопасности

Лекция № 9

Управление ключами. Аппаратные модули безопасности

Рахманенко И.А.

План

- Управление криптографическими ключами
- Концепция иерархии ключей
- Генерация ключей
- Аппаратные модули безопасности

Управление криптографическими ключами

Основной международный стандарт – ISO/IEC 11770 – Key management :

- **Управление ключами** - совокупность процедур и процессов, сопровождающих жизненный цикл ключей в криптосистеме.

Управление криптографическими ключами

Цель управления ключами – обеспечение безопасности криптографических ключей на всех этапах жизненного цикла безопасности всей криптосистемы.

Управление криптографическими ключами

Секретные ключи - необходимо обеспечить секретность, подлинность, целостность:

- Общие секретные ключи симметричных криптосистем;
- Частные секретные ключи асимметричных криптосистем (закрытые ключи).

Открытые ключи - необходимо обеспечить подлинность, целостность:

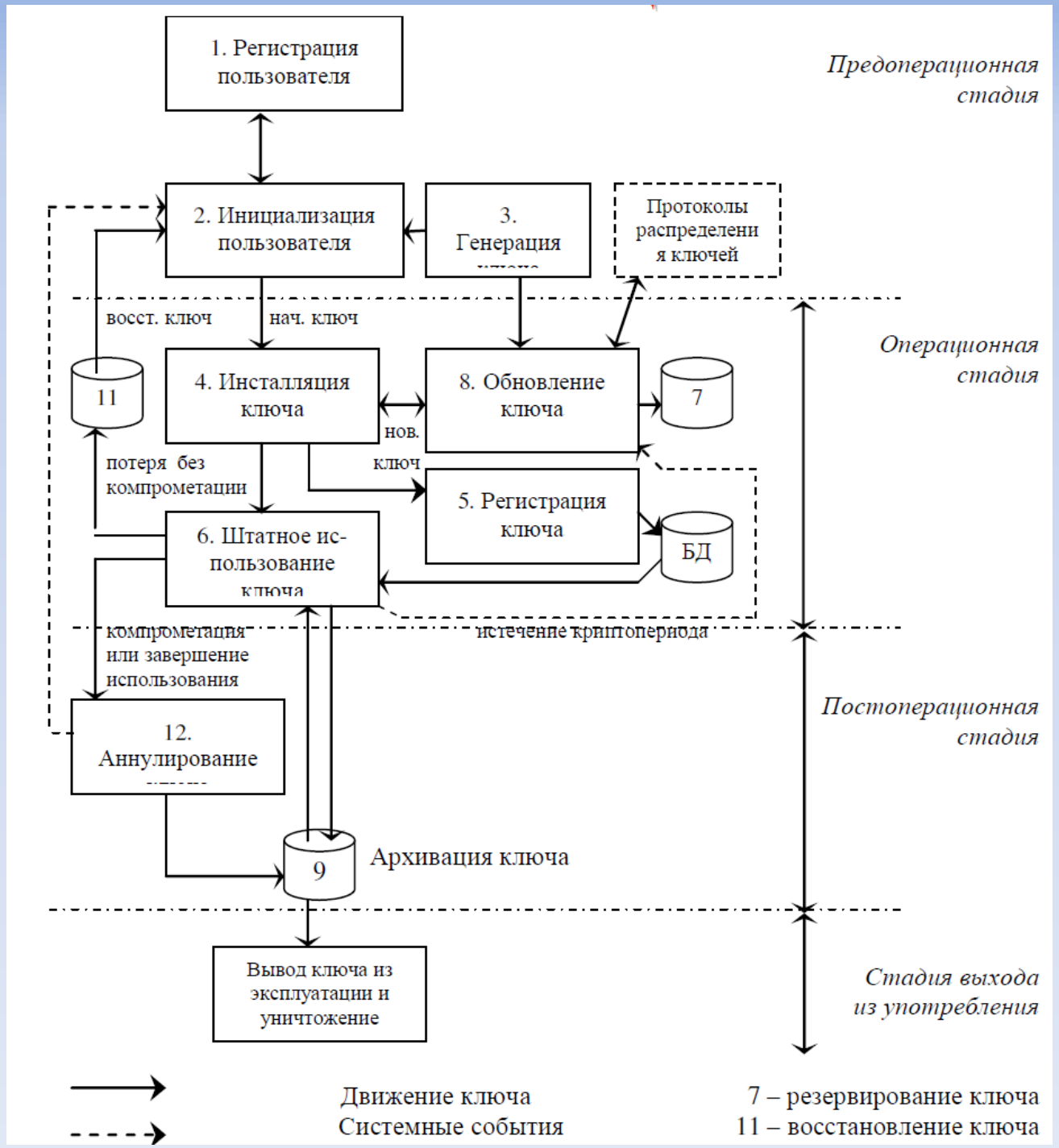
- Открытые ключи асимметричных криптосистем, помещаемые в общедоступные справочники.

Жизненный цикл ключей

- Все криптосистемы, за исключением простейших, в которых используемые ключи зафиксированы раз и навсегда, нуждаются в периодической замене ключей.
- Эта замена проводится с помощью определенных процедур и протоколов, в ряде которых используются и протоколы взаимодействия с третьей стороной.

Жизненный цикл ключей

- Последовательность стадий, которые проходят ключи от момента установления до следующей замены, называется **жизненным циклом** ключей.


1. Регистрация пользователя
Предоперационная стадия
2. Инициализация пользователя
3. Генерация
Протоколы распределения ключей
восст. ключ
нач. ключ
Операционная стадия
11
4. Инсталляция ключа
8. Обновление ключа
7
нов. ключ
потеря без компрометации
5. Регистрация ключа
6. Штатное использование ключа
БД
компрометация или завершение использования
истечение криптопериода
Постоперационная стадия
12. Аннулирование
9
Архивация ключа
Вывод ключа из эксплуатации и уничтожение
Стадия выхода из употребления
Движение ключа
Системные события
7 – резервирование ключа
11 – восстановление ключа

Жизненный цикл ключей

1. **Регистрация пользователей.**

Включает обмен первоначальной ключевой информацией, такой, как общие пароли или PIN-коды, путем личного общения или пересылки через доверенного курьера.

Жизненный цикл ключей

2. **Инициализация.**

Пользователь устанавливает аппаратное оборудование и/или программные средства в соответствии с установленными рекомендациями и правилами.

Жизненный цикл ключей

3. Генерация ключей.

Цель – сделать ключи максимально случайными, непредсказуемыми для противника. Ключи могут генерироваться как самостоятельно пользователем, так и специальным защищенным элементом системы, а затем передаваться пользователю по защищенному каналу.

Жизненный цикл ключей

3. Генерация ключей.

Создание случайных ключей:

- Датчики случайных чисел -физические случайные величины преобразуются в цифровой вид.
- Генераторы псевдослучайных чисел (последовательностей) - числа вырабатываются программами по заранее заданным алгоритмам,, они предсказуемы,, но по своим статистическим качествам очень похожи на случайные.

Жизненный цикл ключей

4. Установка ключей.

Ключи устанавливаются в оборудование тем или иным способом.

Первоначальная ключевая информация, полученная на стадии регистрации пользователей, может либо непосредственно вводиться в оборудование, либо использоваться для установления защищенного канала, по которому передается ключевая информация. Эта же стадия используется в последующем для смены ключевой информации.

Жизненный цикл ключей

5. **Регистрация ключей.**

Ключевая информация связывается регистрационным центром с именем пользователя и сообщается другим пользователям ключевой сети. При этом для открытых ключей создаются сертификационным центром ключевые сертификаты, и эта информация публикуется тем или иным способом.

Жизненный цикл ключей

6. Обычный режим работы.

На этой стадии ключи используются для защиты информации в обычном режиме.

Жизненный цикл ключей

7. Хранение ключа.

Эта стадия включает процедуры, необходимые для хранения ключа в надлежащих условиях, обеспечивающих его безопасность до момента его замены.

Жизненный цикл ключей

7. Хранение ключа.

Главная цель – предотвращение несанкционированного доступа, обеспечение аутентичности ключей.

Как хранить ключ, чтобы его не мог получить злоумышленник?

Жизненный цикл ключей

7. Хранение ключа. Технические средства:

- Токены;
- Смарт-карты – одни из самых удобных и перспективных средств;
- Hardware Security Module (HSM).

Жизненный цикл ключей

7. Хранение ключа. Технические средства:

Преимущества:

- аппаратная реализация криптографических алгоритмов;
- весь ЖЦ ключи изолированы внутри физически защищённой микросхемы;
- существуют критерии оценки защищенности криптографических модулей (американский стандарт FIPS 140-3).

Жизненный цикл ключей

8. Замена ключа.

Замена ключа осуществляется до истечения его срока действия и включает процедуры, связанные с генерацией ключей, протоколами обмена ключевой информацией между корреспондентами, а также с доверенной третьей стороной. Для открытых ключей эта стадия обычно включает обмен информацией по защищенному каналу с сертификационным центром.

Жизненный цикл ключей

9. Архивирование.

В отдельных случаях ключевая информация после её использования для защиты информации может быть подвергнута архивированию для её извлечения со специальными целями (например, рассмотрения вопросов, связанных с отказами от цифровой подписи).

Жизненный цикл ключей

10. Уничтожение ключей.

После окончания сроков действия ключей они выводятся из обращения, и все имеющиеся их копии уничтожаются. При этом необходимо следить, чтобы в случае уничтожения закрытых ключей тщательно уничтожалась и вся информация, по которой возможно их частичное восстановление.

Жизненный цикл ключей

10. Уничтожение ключей.

- **Главная цель** – исключить возможность попадания к посторонним лицам ранее использовавшихся ключей.
- Криптографические ключи нельзя просто вывести из употребления – необходимо физически уничтожить все копии ключей из памяти аппаратных средств криптографической защиты.

Жизненный цикл ключей

11. Восстановление ключей.

Если ключевая информация уничтожена, но не скомпрометирована (например, из-за неисправности оборудования или из-за того, что оператор забыл пароль) должны быть предусмотрены меры, дающие возможность восстановить ключ из хранимой в соответствующих условиях его копии.

Жизненный цикл ключей

12. Отмена ключей.

В случае компрометации ключевой информации возникает необходимость прекращения использования ключей до окончания срока их действия. При этом должны быть предусмотрены необходимые меры оповещения абонентов сети. При отмене открытых ключей, снабженных сертификатами, одновременно производится прекращение действия сертификатов.

Распространение ключей

Транспортировка - самый опасный этап !

- Для секретных ключей симметричных криптосистем главная цель – предотвратить попадание ключи к посторонним лицам: традиционные меры физической защиты, усиленные аппаратными и организационными мерами.
- Для открытых ключей главная цель – обеспечить подлинность и целостность сложная задача, которая решается созданием инфраструктуры открытых ключей.

Распространение ключей

Инфраструктура открытых ключей (PKI – Public Key Infrastructure) – универсальная модель организованной поддержки криптографических средств защиты информации в крупномасштабных компьютерных системах в соответствии с принятыми в них политиками безопасности, которая реализует управление криптографическими ключами на всех этапах их жизненного цикла, обеспечивая взаимодействие всех средств защиты.

Концепция иерархии ключей

- Любая информация об используемых ключах должна быть защищена - храниться в зашифрованном виде.
- Необходимость в хранении и передаче ключей, зашифрованных с помощью других ключей, приводит к концепции иерархии ключей.

Концепция иерархии ключей

- В стандарте ISO 8532 (Banking-Key Management) подробно изложен метод главных сеансовых ключей (master/session keys).
- Суть метода состоит в том, что вводится иерархия ключей: главный ключ (ГК), ключ шифрования ключей (КК), ключ шифрования данных (КД)

Концепция иерархии ключей

Иерархия ключей может быть:

- двухуровневой (КК/КД);
- трехуровневой (ГК/КК/КД).

Ключи более высоких уровней используются для защиты ключей или данных на более низких уровнях, что уменьшает ущерб при раскрытии ключей и объём необходимой информации, нуждающейся в физической защите.

Концепция иерархии ключей

- Нижний уровень: **рабочие или сеансовые КД**.
- Применяются для шифрования данных, персональных идентификационных номеров (PIN) и аутентификации сообщений.

Концепция иерархии ключей

- **Ключи шифрования ключей (КК)**.
- Используют для шифрования ключей с целью защиты при передаче или хранении.
- Никогда не должны использоваться как сеансовые КД.

Концепция иерархии ключей

- **Ключи шифрования ключей (КК)**.
- КК, используемые для пересылки ключей между двумя узлами сети, называются ключами обмена между узлами сети (cross domain keys).
- В большинстве случаев в канале применяются два ключа для обмена между узлами сети, по одному в каждом направлении. Поэтому каждый узел сети будет иметь ключ отправления для обмена с узлами сети и ключ получения для каждого канала, поддерживаемого другим узлом сети.

Концепция иерархии ключей

- Верхний уровень **- главный ключ или мастер-ключ (ГК)**.
- Шифрует КК, если требуется сохранить его на диске.
- Обычно в одной системе используется только один мастер-ключ.
- Для исключения перехвата мастер-ключ распространяется между участниками обмена неэлектронным способом.

Концепция иерархии ключей

- Верхний уровень **- главный ключ или мастер-ключ (ГК)**.
- Значение мастер-ключа сохраняется длительное время (до нескольких недель или месяцев). Мастер-ключ компьютера создается случайным выбором из всех возможных значений ключей и помещается в защищенный от считывания и записи блок криптографической системы.

Концепция иерархии ключей

- Рабочие ключи (например, сеансовый) создаются с помощью генератора случайных чисел и могут храниться в незащищенном месте, поскольку такие ключи генерируются в форме криптограмм (генератор выдает вместо ключа К его криптограмму Е (К), получаемую с помощью мастер-ключа.
- Расшифровывание такой криптограммы осуществляется перед применением ключа К.

Концепция иерархии ключей

- Пример: зашифрованные рабочие ключи находятся вместе с данными, ключи шифрования ключей хранятся в системе.
- Главный ключ находится на eToken. Для расшифровывания данных обязательно наличие этого ключа.

Сроки действия ключей

- Срок действия ключа означает промежуток времени, в течение которого он может быть использован доверенными сторонами.

Сроки действия ключей

Сокращение сроков действия ключей необходимо для достижения следующих целей:

- ограничения объёма информации, зашифрованной на данном ключе, которая может быть использована для криптоанализа;
- ограничения размера ущерба при компрометации ключей;
- ограничения объёма машинного времени, которое может быть использовано для криптоанализа.

Сроки действия ключей

Выделяют:

- Ключи с длительным сроком действия. К ним относится главный ключ, часто — ключи для шифрования ключей.
- Ключи с коротким сроком действия. К ним относятся ключи для шифрования данных.

Сроки действия ключей

- Как правило, в телекоммуникационных приложениях используются ключи с коротким сроком действия, а для защиты хранимых данных — с длительным сроком действия.
- «Короткий срок действия» относится только к сроку действия ключа, а не к промежутку времени, в течение которого ключ должен оставаться в секрете.

Сроки действия ключей

- Например, к ключу, используемому для шифрования в течение только одного сеанса связи, часто предъявляется требование, чтобы зашифрованная на нём информация не могла быть вскрыта на протяжении нескольких десятков лет.
- В то же время электронная подпись проверяется немедленно после передачи сообщения, поэтому ключ подписи должен сохраняться в тайне в течение достаточно короткого срока.

Генерация случайных чисел

- Нужны для генерации ключей шифрования, должны удовлетворять определенным требованиям.
- Генератор псевдослучайных чисел.
- Аппаратный генератор случайных чисел.

Требования к ГСЧ

- Требуемое «качество» случайности меняется от задачи к задаче.
- Например, генерация одного случайного числа в некоторых протоколах требует только уникальности, тогда как генерация мастер-ключа или одноразового шифроблокнота требует высокой энтропии.
- В идеале, генерация случайных чисел в КСГПСЧ использует высоконадёжный источник энтропии, которым может быть аппаратный генератор случайных чисел или ход непредсказуемых процессов в системе — хотя в обоих случаях возможны уязвимости.

Требования к ГСЧ

- Криптографически стойкий ГПСЧ должен удовлетворять «тесту на следующий бит».
- Смысл теста: не должно существовать полиномиального алгоритма, который, зная первые k битов случайной последовательности, сможет предказать (k+1)-ый бит с вероятностью более 50 %.
- Эндрю Яо доказал в 1982 году, что генератор, прошедший «тест на следующий бит», пройдёт и любые другие статистические тесты на случайность, выполнимые за полиномиальное время.

Требования к ГСЧ

- КСГПСЧ должен оставаться надёжным даже в случае, когда часть или все его состояния стали известны (или были корректно вычислены).
- Это значит, что не должно быть возможности получить случайную последовательность, созданную генератором, предшествующую получению этого знания криптоаналитиком.
- Кроме того, если во время работы используется дополнительная энтропия, попытка использовать знание о входных данных должна быть вычислительно невозможна.

Требования к ГСЧ

- Большинство генераторов псевдослучайных чисел не подходят для использования в качестве КСГПСЧ по обоим критериям.
- Во-первых, несмотря на то, что многие ГПСЧ выдают последовательность случайную с точки зрения разнообразных статистических тестов, они не надёжны по отношению к обратной разработке. Могут быть обнаружены специализированные, особым образом настроенные тесты, которые покажут, что случайные числа, получаемые из ГПСЧ не являются по настоящему случайными.

Требования к ГСЧ

- Во-вторых, для большинства ГПСЧ возможно вычислить всю псевдослучайную последовательность, если их состояние скомпрометировано, что позволит криптоаналитику получить доступ не только к будущим сообщениям, но и ко всем предыдущим. КСГПСЧ разрабатываются с учётом сопротивляемости к различным видам криптоанализа.

Псевдослучайный ГСЧ

- Генератор псевдослучайных чисел — алгоритм, порождающий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению (обычно равномерному).

Достоинства:

- Требуется однократная проверка;
- Многократная воспроизводимость последовательности чисел;
- Мало места в памяти и нет внешних устройств.

Недостатки:

- Запас чисел ограничен периодом последовательности;
- Затраты машинного времени.

Псевдослучайный ГСЧ

Рассмотрим три класса реализации КСГПСЧ:

1. На основе криптографических алгоритмов (хэш-функция, потоковые шифры)
2. На основе вычислительно сложных математических задач
3. Специальные реализации (в разных ОС)

Аппаратный ГСЧ

- Аппаратный ГСЧ (генератор истинно случайных чисел) — устройство, которое генерирует последовательность случайных чисел на основе измеряемых, хаотически изменяющихся параметров протекающего физического процесса.
- Основаны на использовании надёжных источников энтропии: тепловой шум, дробовой шум, фотоэлектрический эффект, квантовые явления и т. д.

Аппаратный ГСЧ

Достоинства:

- Запас чисел не ограничен;
- Расходуется мало операций;
- Не занимается место в памяти.

Недостатки:

- Требуется периодическая проверка;
- Нельзя воспроизводить последовательности;
- Используется специальное устройство;
- Необходимы меры по обеспечению стабильности.

Хранение ключей

- Важные ключи нельзя хранить локально -> возможна утечка ключа.

Возможно применение внешних устройств для хранения ключей и выполнения криптографических операций:

- eToken и подобные;
- Аппаратные модули безопасности.

Аппаратные модули безопасности

- Аппаратный модуль безопасности (hardware security module - HSM) – вычислительное устройство, которое обеспечивает безопасность и управляет криптографическими ключами, используемыми для усиленной аутентификации и криптографических функций.

Аппаратные модули безопасности

Функции:

- Безопасная генерация ключей шифрования
- Безопасное хранение и управление ключами
- Работа с зашифрованной и конфиденциальной информацией
- Работа с симметричной и асимметричной криптографией.

Аппаратные модули безопасности

Применение:

- PKI, центр сертификации
- Банковские операции
- Установление SSL соединений

Безопасный криптопроцессор

- Используют безопасный криптопроцессор для выполнения криптографических операций.
- Безопасный криптопроцессор - это система на кристалле или микропроцессор, предназначенный для проведения криптографических операций и обеспеченный мерами физической защиты, дающими ему некоторую возможность противодействия несанционированному доступу.

Безопасный криптопроцессор

- В отличие от криптографических процессоров, "доверяющих" шине и выводящих незашифрованные данные на нее, как будто она находится в защищенной среде, безопасный криптопроцессор не выводит незашифрованные данные или незашифрованные программные инструкции в среду, которая не может быть гарантированно защищенной все время.

Безопасный криптопроцессор

Особенности:

- Обнаружение подделок и индикация вскрытия.
- Проводящие защитные слои в чипе, мешающие считывать внутренние сигналы.
- Контролируемое исполнение, чтобы предотвратить раскрытие любой секретной информации по временным задержкам.
- Автоматическое обнуление секретов в случае фальсификации.

Безопасный криптопроцессор

Особенности:

- Доверенный загрузчик - проверяет подлинность операционной системы перед ее запуском.
- Доверенная операционная система - проверяет подлинность приложений перед их запуском.
- Аппаратные регистры, где реализуется модель с разделением привелегий.

Аппаратные модули безопасности

- Может иметь несколько уровней физической защиты в одном чипе криптопроцессоре.
- Чип криптопроцессора может быть помещен аппаратный модуль безопасности наряду с другими процессорами и памятью, где хранятся и обрабатываются зашифрованные данные.

Аппаратные модули безопасности

- Любая попытка извлечь его вызовет обнуление ключей в крипточипе.
- Аппаратные модули безопасности также могут быть частью компьютера (например банкомата), который проводит операции внутри запертого сейфа, чтобы предотвратить кражи, замены и подделки.

Аппаратные модули безопасности. Примеры

- Атликс HSM
- КриптоПро HSM
- ViPNet HSM
- Другие.

Атликс HSM

- Атликс HSM - аппаратный криптографический модуль (hardware security module), совместимый с КриптоПро CSP.
- Предназначен для обеспечения безопасного хранения и использования закрытого ключа уполномоченного лица удостоверяющего центра

Атликс HSM

Криптографические алгоритмы, реализуемые криптомодулем **Атликс HSM**:

- генерация ключей, используемых в алгоритмах ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001;
- шифрование/расшифрование данных по ГОСТ 28147-89;
- контроль целостности данных посредством вычисления имитовставки по ГОСТ 28147-89;
- вычисление значения хэш-функции в соответствии с ГОСТ Р 34.11-94;

Атликс HSM

Сроки действия ключей, при использовании криптомодуля **Атликс HSM:**

- максимальный срок действия закрытых ключей ЭЦП - 5 лет;
- максимальный срок действия открытых ключей ЭЦП при использовании алгоритма ГОСТ Р 34.10-2001 - 30 лет.

КриптоПро HSM

- КриптоПро HSM - программно-аппаратный криптографический модуль (hardware security module), совместимый с КриптоПро CSP.

КриптоПро HSM

Функции:

- создание и проверка электронной цифровой подписи;
- вычисление хэш-функции;
- шифрование и расшифрование блоков данных;
- вычисление имитовставки блоков данных;
- генерация и защищенное хранение ключевой информации (все ключи хранятся в зашифрованном виде);
- управление учетными записями пользователей криптографического сервиса.

КриптоПро HSM

Сроки действия ключей, при использовании ПАКМ КриптоПро HSM:

- максимальный срок действия закрытых ключей ЭЦП - до 3-х лет;
- максимальный срок действия закрытых ключей ЭЦП при использовании ПАКМ в качестве СКЗИ в программных комплексах удостоверяющих центров, реализованных и сертифицированных по классу защиты КВ2 - до 7-и лет;
- максимальный срок действия открытых ключей ЭЦП при использовании алгоритма ГОСТ Р 34.10-2001 - 30 лет;
- максимальный срок действия открытых ключей обмена – до 3-х лет;
- максимальный срок действия закрытого ключа обмена совпадает со сроком действия закрытого ключа.

КриптоПро HSM

Применение:

- в серверных компонентах распределенных систем, требующих высокую степень защиты ключа ЭЦП, например в программно-аппаратных комплексах Удостоверяющих центров;
- в дополнительных службах удостоверяющих центров: в службах штампов времени; в службах актуальных статусов сертификатов; в службах электронного нотариата;

КриптоПро HSM

Применение:

- В сетях передачи конфиденциальной информации для реализации протокола TLS: в web-серверах; в серверах баз данных; в серверах приложений;
- в персональных (не серверных) системах, где требуется высокий уровень защиты ключевой информации.

Рассмотренные вопросы

- Управление криптографическими ключами
- Концепция иерархии ключей
- Генерация ключей
- Аппаратные модули безопасности

СПАСИБО ЗА ВНИМАНИЕ!