Криптографические методы как часть общей системы защиты информации

Введение

Рассмотрим применение средств криптографии в общей системе защиты автоматизированных информационных систем.

Темы для обсуждения

- Симметричное шифрование
- Шифрование с открытым ключом
- Средства ЭЦП
- Инфраструктура открытых ключей
- Защита криптографических систем

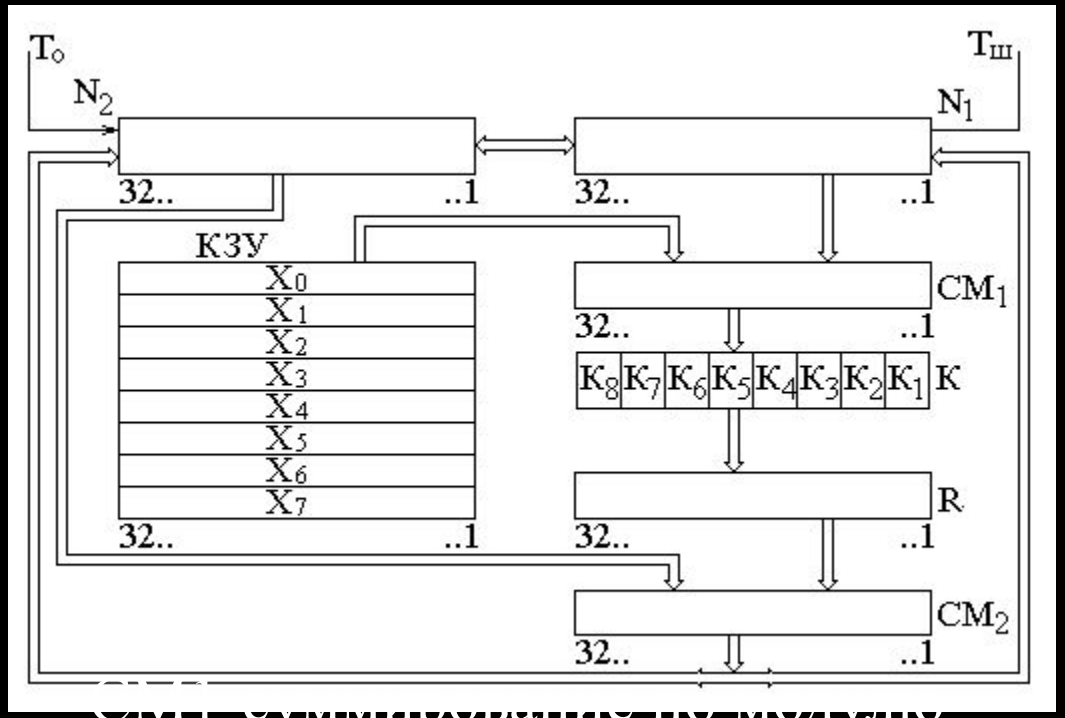
Симметричное шифрование и возможные атаки

Режимы шифрования ГОСТ 28147-89

-простая замена;
-гаммирование;
-гаммирование с обратной связью;
-вычисление имитовставки.

Режим простой замены (электронная кодировочная книга)

- Каждый блок исходного текста шифруется блочным шифром независимо от других;
- Стойкость режима равна стойкости самого шифра. Возможно простое распараллеливание вычислений;
- Скорость шифрования равна скорости блочного шифра;
- Недостаток - нельзя скрыть структуру исходного текста.

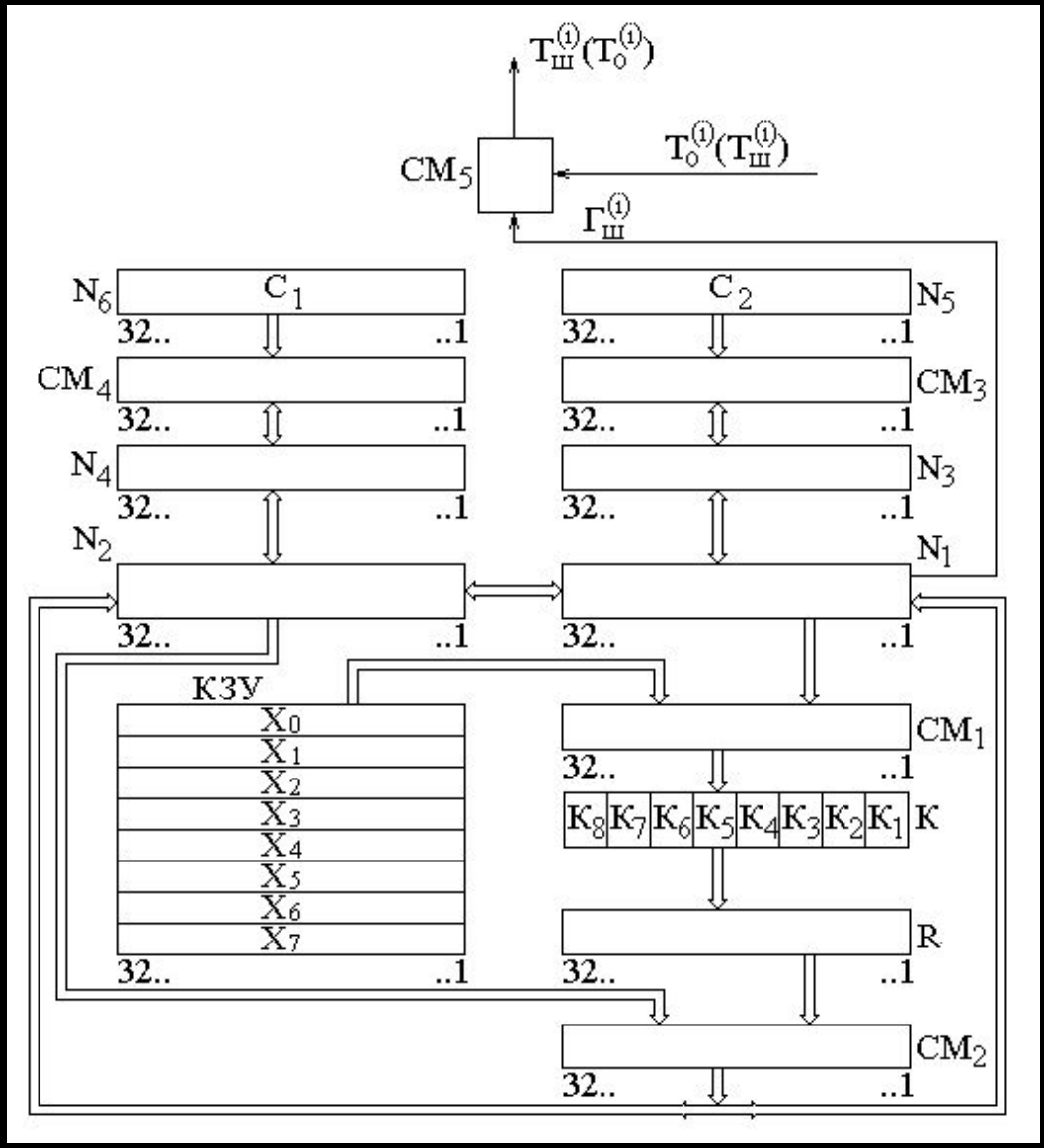


СМ1-суммирование по модулю 32

СМ2-суммирование по модулю 2

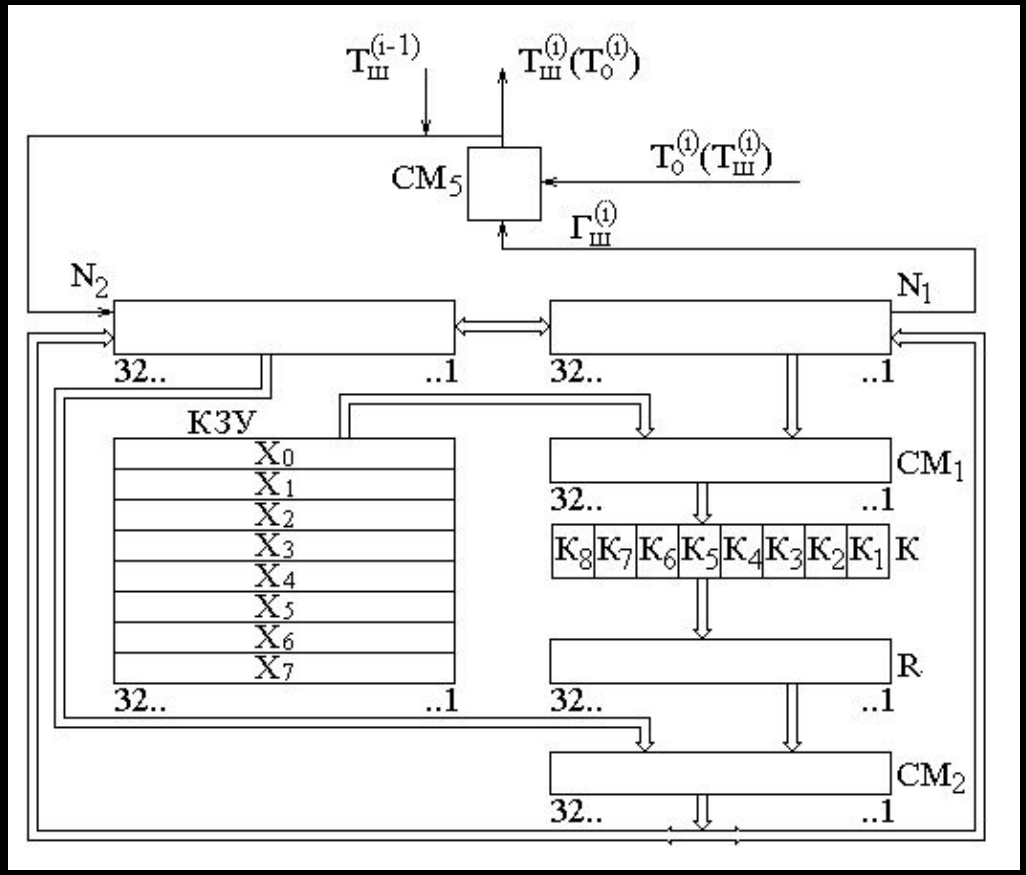
Гаммирование

- Каждый бит открытого текста складывается поразрядно по модулю 2 с специально вырабатываемой гаммой шифра.
- Для начала процесса шифрования используется начальный вектор, который передается в канал связи в открытом виде.
- Имеет более высокую стойкость, чем РПЗ, поскольку становится невозможным прямое манипулирование исходным текстом.
- Скорость равна скорости блочного шифра.


$T_{ш}^{(i)}(T_{о}^{(i)})$
$T_{о}^{(i)}(T_{ш}^{(i)})$
$СМ_5$
$Г_{ш}^{(i)}$
N_6
C_1
C_2
N_5
32..
..1
$СМ_4$
$СМ_3$
N_4
N_3
N_2
N_1
КЗУ
X_0
X_1
X_2
X_3
X_4
X_5
X_6
X_7
$СМ_1$
$К_8$ $К_7$ $К_6$ $К_5$ $К_4$ $К_3$ $К_2$ $К_1$ К
R
$СМ_2$

Гаммирование с обратной связью

- Предыдущий блок шифрованного текста вводится еще раз и для получения очередного блока шифрованного текста результат складывается с блоком исходного текста;
- Для начала процесса шифрования требуется начальный вектор;
- Стойкость режима равна стойкости самого шифра. Не позволяет производить простое распараллеливание;
- Структура исходного текста скрывается. Манипулирование начальным и конечным блоками становится невозможным;
- Скорость равна скорости блочного шифра.


$T_ш^{(i-1)}$
$T_ш^{(i)}(T_o^{(i)})$
$T_o^{(i)}(T_ш^{(i)})$
$СМ_5$
$Г_ш^{(i)}$
N_2
N_1
32..
..1
32..
..1
КЗУ
X_0
X_1
X_2
X_3
X_4
X_5
X_6
X_7
32..
..1
$СМ_1$
32..
..1
K_8 K_7 K_6 K_5 K_4 K_3 K_2 K_1 K
R
32..
..1
$СМ_2$
32..
..1

Преимущества симметричного шифрования

- высокая скорость работы;
- хорошо проработанная теоретическая база.

Недостатки

- Сложности с сохранением ключей в секрете, если в системе много пользователей

Управление криптографическими ключами симметричного шифрования

Жизненный цикл ключей:

генерация ключей,
регистрация пользователей и ключей,
инициализация ключей,
период действия,
хранение ключа,
замена ключа,
архивирование,
уничтожение ключей,
восстановление ключей,
отмена ключей.

Генерация ключей

- Нет нормативной базы
- Не все ключи равноценны
- Не ясно что делать с блоком подстановки

Атаки на системы симметричного шифрования

- На открытый текст;
- На алгоритм шифрования (криптоанализ);
- На ключи шифрования.

Криптоанализ

- Метод взлома «грубой силы»;
- Линейный анализ;
- Дифференциальный анализ.

Основывается на статистических особенностях, присущих открытому тексту и шифртексту

Криптография с открытым ключом

Используются два ключа, составляющие уникальную пару.

Один хранится в секрете, а другой, открытый, свободно распространяется.

Требования к алгоритму

- Для отправителя **A** не должен вызывать вычислительных трудностей процесс создания шифрованного текста при наличии открытого ключа и сообщения M, которое требуется зашифровать;
- Для получателя **B** не должен вызывать вычислительных трудностей процесс расшифрования полученного шифрованного текста с помощью личного ключа;
- Для противника должно быть невозможным, с точки зрения вычислительных возможностей, восстановление оригинального сообщения из имеющегося открытого ключа и шифрованного текста;
- функции зашифрования и расшифрования можно применять в любом порядке .

Схема применения и возможные атаки

Преимущества

- Снимается проблема с хранением одинаковых ключей у многих пользователей

Недостатки

- Малая скорость работы

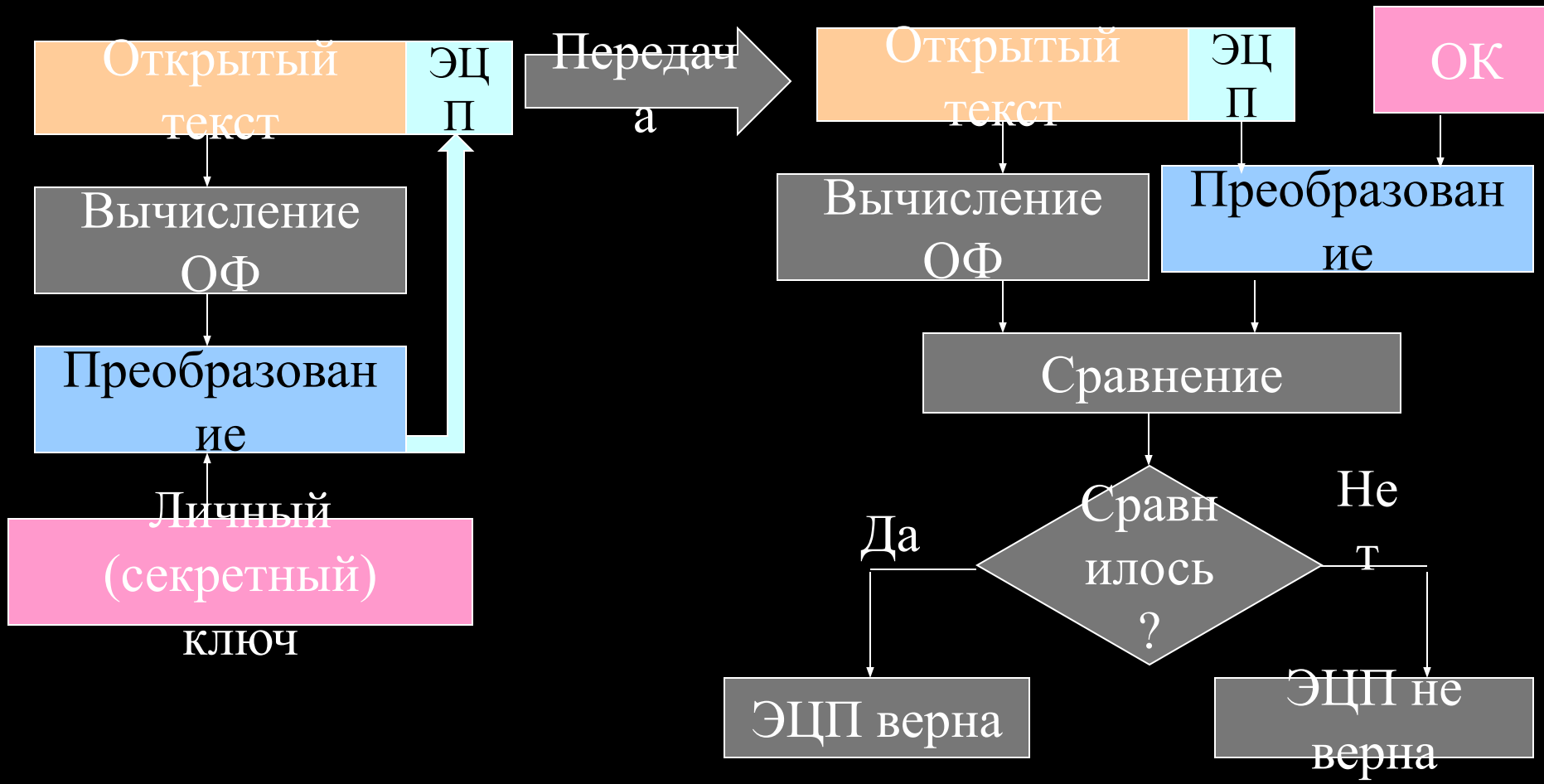
Применение

- Шифрование ключей для симметричных систем;
- Электронно-цифровая подпись

Однонаправленная функция

Под *однонаправленной будем* понимать эффективно вычислимую функцию, для обращения которой (т.е. для поиска хотя бы одного значения аргумента по заданному значению функции) не существует эффективных алгоритмов

Схема применения ЭЦП в электронном документе



5 Процедура выработки ЭЦП

5.1 Исходные данные и параметры

5.1.1 В процедуре выработки ЭЦП используются следующие исходные параметры: *p*, *l*, *q*, *r* и *a* − числа, генерируемые процедурами, описанными в разделе 7, и являющиеся открытыми параметрами.

5.1.2 Исходными данными для процедуры выработки ЭЦП являются:

M − последовательность чисел *M=(m1, m2, …, mz),* где для *i=1, 2, …, z* и *z* – длина последовательности *M*;

x – целое число, $0 < x < q$, являющееся личным ключом подписи и хранящееся в тайне, где *q* – параметр, определяемый в разделе 7.

5.2 Используемые переменные

- В процедуре выработки ЭЦП используются следующие переменные:
- *k* – целое число, , которое хранится в тайне и должно быть уничтожено сразу после использования;
- *t* – целое число, $0 < t < p$;
- *Mt* – последовательность чисел из *Z(8),* имеющая конечную длину;
- *U* – целое число, ;
- *V* – целое число, ;
- *S* – целое число, .

5.3 Алгоритм выработки ЭЦП

- 1 Выработать с помощью физического датчика случайных чисел или псевдослучайным методом с использованием секретных параметров число k $(1<k<q)$;
- 2 $t:=a^{(k)}$;
- 3 Представить число t в виде разложения по основанию 2^8:
- $t=\Sigma t_i*(2^8)^i$;;
- 4 $Mt:=(t_0,t_1,\ldots t_{n-1},m_1,\ldots,m_z\};$
- 5 $U:=h(M)$.
- Если $U = 0$, то перейти к шагу 1;
- 6 $V:=(k - x*U) \bmod q$.
- Если $V = 0$, то перейти к шагу 1;
- 7 $S:=U*2r+V$.
- ЭЦП последовательности M является число S.

Вопросы:

- Можно ли гарантировать на ПЭВМ целостность программ, реализующих криптоалгоритмы?
- Можно ли надежно хранить секретные ключи на ПЭВМ?
- Как быть уверенным в том, что открытый ключ, полученный Вами не искажен?

Инфраструктура Открытых Ключей (PKI)

Основана на:

- Использовании электронного документа для хранения ОК;
- Надежном хранении корневого сертификата доверенной стороной;
- Удостоверении правильности хранимых сертификатов или
- Подтверждении факта его недействительности (компрометации)

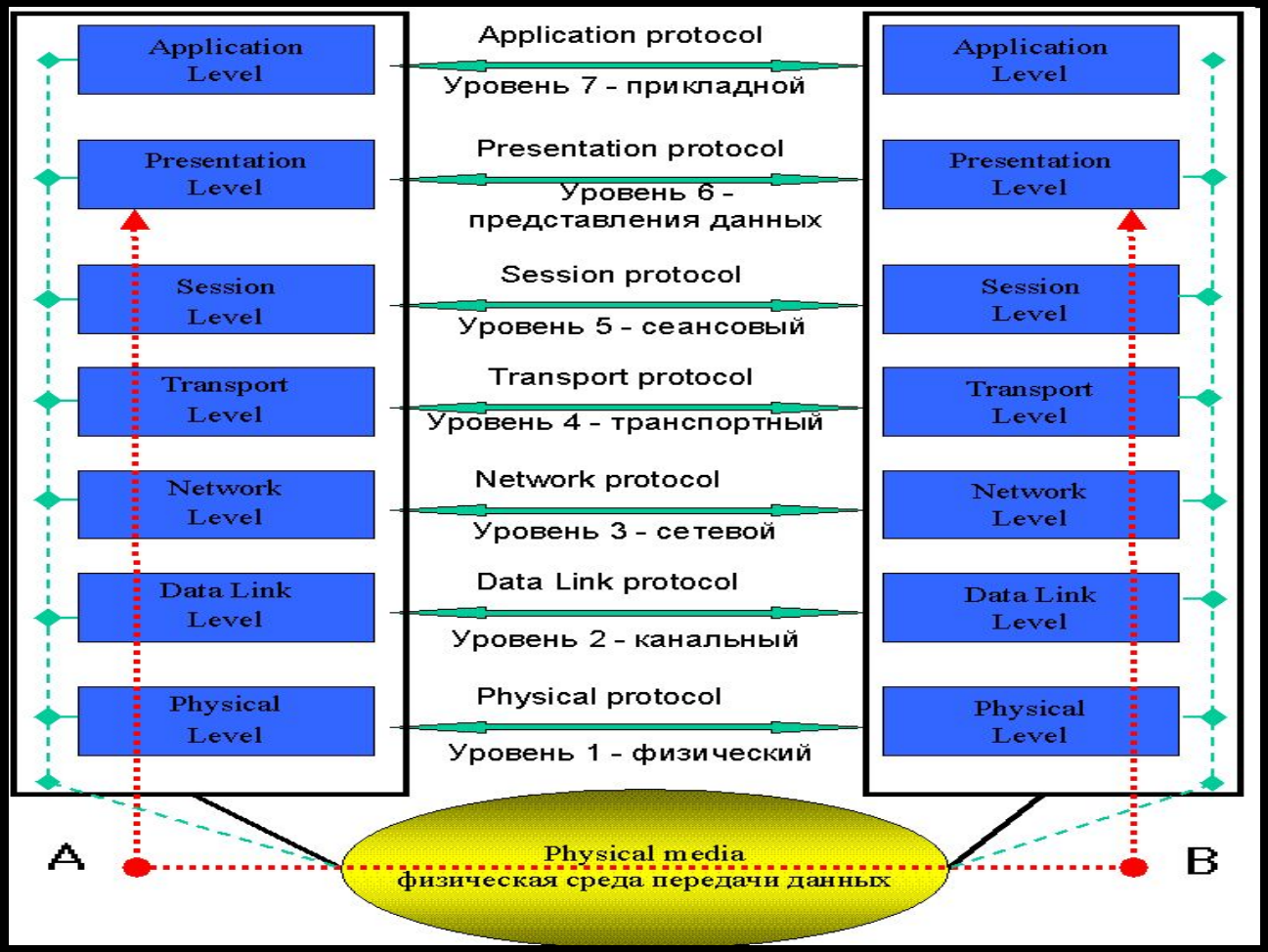
Центры сертификации

- Создают сертификаты;
- Обеспечивают надежное хранение главного – корневого сертификата;
- Извещают о недействительности (ведут списки отозванных сертификатов)

Алгоритмы защищенного обмена

- SSL (SSH, HTTPS)
- IPSec
- и многие другие

Модель ISO/OSI



Как это выглядит на деле для TCP/IP?

Прикладной (П+ПД+Сеанс)

Транспортный

Сетевой

Сетевого доступа (К+Ф)

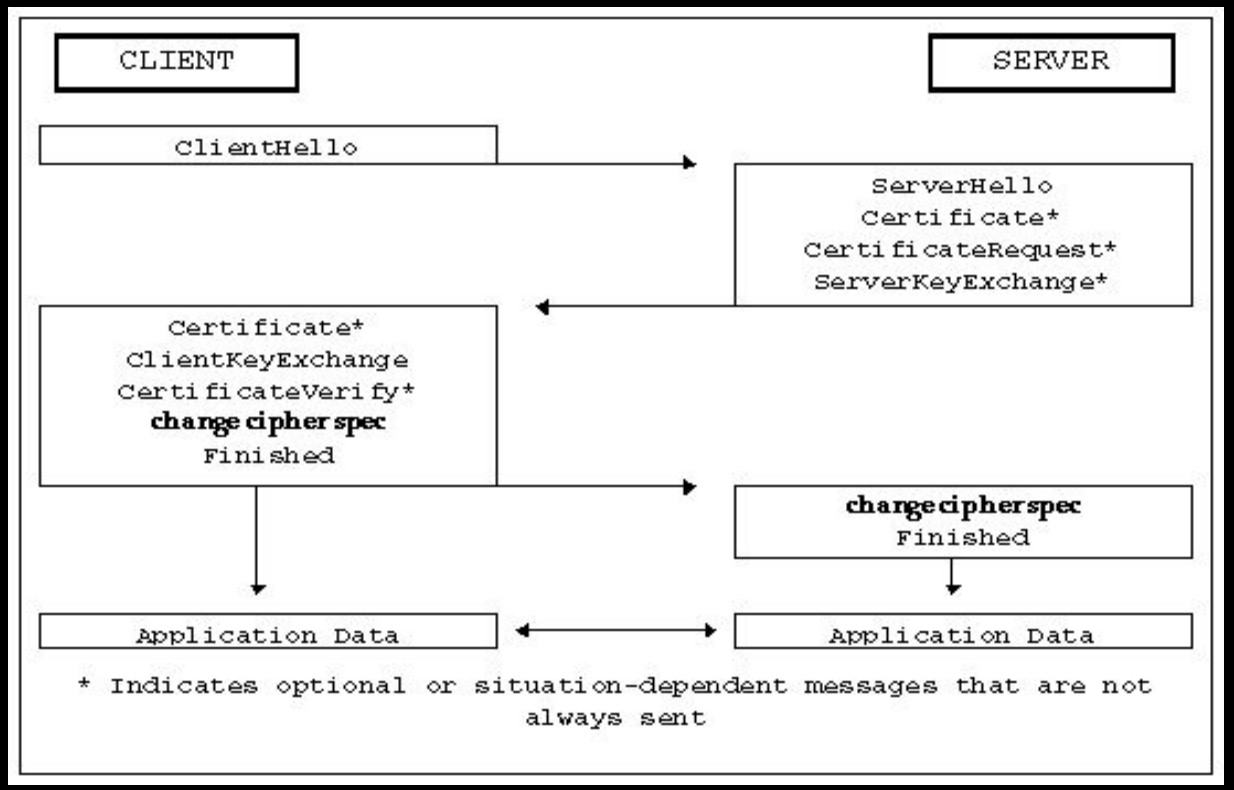
Secret Socket Layer (SSL)

- Два уровня (транспортный уровень модели ISO/OSI):

  1) Уровень установления соединения (согласование криптографических параметров – подготовка защищенного соединения);

  2) Уровень записи данных приложения (передача данных в защищенном канале).

Уровень установления соединения



Архитектура IPsec

Протокол AH

Аутентифицирующий заголовок (AH) является обычным опциональным заголовком и, как правило, располагается между основным заголовком пакета IP и полем данных. Наличие AH никак не влияет на процесс передачи информации транспортного и более высокого уровней. Основным и единственным назначением AH является обеспечение защиты от атак, связанных с несанкционированным изменением содержимого пакета, и в том числе от подмены исходного адреса сетевого уровня. Протоколы более высокого уровня должны быть модифицированы в целях осуществления проверки аутентичности полученных данных

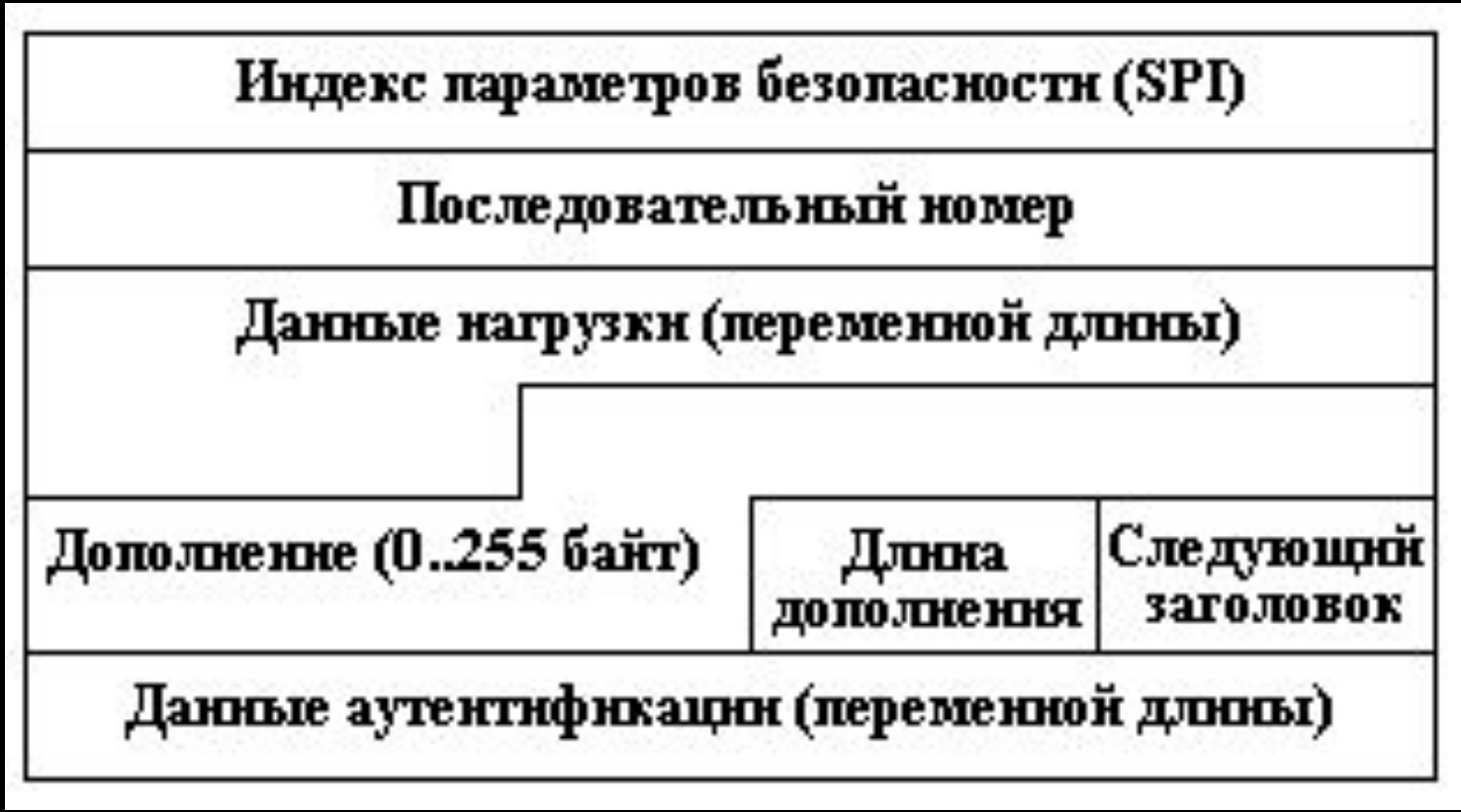
Формат АН


Следующий заголовок
Длина нагрузки
Зарезервировано
Индекс параметров безопасности
Поле последовательного номера
Данные аутентификации (переменной длины)

Протокол ESP

Используется для инкапсуляции зашифрованных данных. Заголовок ESP является последним в ряду опциональных заголовков, "видимых" в пакете. Поскольку возможно применение разных криптоалгоритмов, формат ESP может претерпевать значительные изменения. Тем не менее, всегда присутствуют следующие обязательные поля: SPI, указывающее на контекст безопасности и Sequence Number Field, содержащее последовательный номер пакета. Поле "ESP Authentication Data" (контрольная сумма), не является обязательным в заголовке ESP. Получатель пакета ESP расшифровывает ESP заголовок, использует параметры и данные применяемого алгоритма шифрования для декодирования информации.

Вид заголовка ESP



Наши реквизиты:

г.Минск, ул. Первомайская, 17

Тел. 294-76-76, 233-95-68

eMail: kontakt@mail.bn.by