М. М. Грунтович, С. Н. Семкин

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА В СИСТЕМЕ СОПРОВОЖДЕНИЯ И УПРАВЛЕНИЯ НАЗЕМНЫМИ ТРАНСПОРТНЫМИ СРЕДСТВАМИ

1. Состав и назначение ПКЗИ

Система сопровождения и управления наземными транспортными средствами позволяет осуществлять навигационный мониторинг транспортных средств (ТС) с использованием спутниковых систем навигации GPS/GLONASS для получения текущих координат ТС и систем сотовой связи в формате GSM/GPRS для передачи оперативных данных, включая координаты местоположения ТС, от ТС к диспетчерскому центру (ДЦ). Для решения этой задачи их аппаратные бортовые комплексы (БК), наряду с приемопередатчиками и модемами систем GPS/GLONASS и GSM, содержат бортовой микроконтроллер (БМ), являющийся их ядром. БМ осуществляет формирование пакетов сообщений, отправляемых на ДЦ, в том числе текущие значения координат ТС и показаний интегрированных в систему датчиков, хранение этих пакетов в течение времени, когда они не могут быть отправлены по причине выхода ТС за зону действия сотовой связи.

В системе выделены ДЦ, так называемый федеральный диспетчерский центр (ФДЦ) и необходимое количество региональных ДЦ (РДЦ). Каждый ДЦ осуществляет получение переданной БК информации, ее предварительную обработку и передачу в базу данных, из которой эта информация поступает на обработку в центр обработки (ЦО).

В данной статье речь пойдет о реализации криптографической защиты сообщений, передаваемых между БК и ДЦ. Подсистема криптографической защиты информации (ПКЗИ) включает в себя программные модули программного обеспечения БМ, ДЦ и ЦО, а также центр управления ключами (ЦУК), который выполняет необходимые функции управления ключевой системой остальных компонентов.

Цель ПКЗИ — безопасная передача коротких сообщений между БК и одним из ДЦ с обеспечением аутентификации, конфиденциальности и контроля целостности.

Архитектура связей в системе изображена на рис. 1.

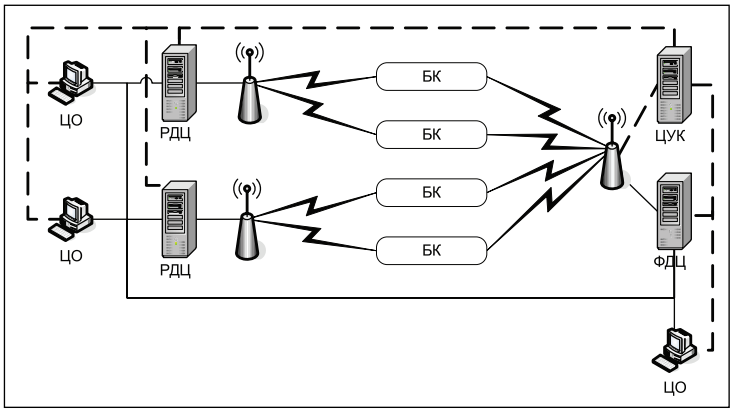

Рис. 1. Архитектура ПКЗИ

При передаче сообщения от БК в ДЦ подписываются и шифруются. Сообщения от ДЦ к БК шифруются. Целостность сообщений от ДЦ к БК обеспечивается с помощью имитовставки по ГОСТ 28147 [1].

ДЦ, получив сообщение от БК, расшифровывает его, проверяет цифровую подпись и передает вместе с подписью на обработку в ЦО.

БК, получив сообщение от ДЦ, расшифровывает его, проверяет имитовставку.

ЦО перед обработкой сообщения от БК проверяет его цифровую подпись.

БК и ДЦ снабжаются рабочими ключами шифрования и цифровой подписи, обеспечивающими защиту сообщений между собой. ЦУК выполняет регистрацию всех БК и ДЦ (снабжение базовыми ключами) и регулярное обновление рабочих ключей.

ЦО обладают только базой открытых ключей цифровой подписи БК, а также базовым открытым ключом ЦУК, подписывающим сертификаты открытых ключей БК.

Собственная ключевая информация (КИ) ЦУК, ДЦ и ЦО сохраняется на внешних носителях КИ, которыми служат аппаратные модули «Аккорд-У» и ПСКЗИ ШИПКА.

В ПКЗИ применяются алгоритмы шифрования по ГОСТ 28147 [1], цифровой подписи по ГОСТ Р 34.10 [2], хэширования по ГОСТ Р 34.11 [3].

2. Ключевая система управления ключами

Для установления/смены ключей защиты сообщений используется система управления ключами, которая, в свою очередь, обладает базовыми долговременными криптографическими ключами. Протоколы управления ключами между БК и ЦУК обеспечивают аутентификацию, конфиденциальность и целостность, используя ключи управления ключами, описанные далее.

Секретные ключи защиты сообщений управления ключами между БК и ЦУК вычисляются на основе секретного базового мастер-ключа управления ключами MKEK, который генерируется при инициализации ЦУК с помощью физического ДСЧ и сохраняется во внутренней памяти аппаратного модуля «Аккорд-У».

Для смены ключей БК используется ключ управления ключами $KEK_{БК}$, который вычисляется из мастер-ключа управления ключами MKEK следующим образом:

$$KEK_{БК} = F(MKEK, Id_{БК}). \quad (1)$$

Ключ $KEK_{БК}$ записывается в БК при его регистрации в ЦУК. Смена этого ключа возможна только при повторной регистрации. ЦУК может вычислять этот ключ непосредственно перед выполнением операций защиты протокола управления ключами или сохранять во внешней памяти.

Для защиты сообщений управления ключами, переданных/принятых в день d между ЦУК и БК, используется производный ключ $KEK_{БК}^{d}$, вычисляемый следующим образом:

$$KEK_{БК}^{D} = F(KEK_{БК}, d). \quad (2)$$

3. Ключевая система шифрования сообщений

Для защиты конфиденциальности связи БК и ДЦ используется система производных ключей.

Секретные ключи шифрования сообщений между ДЦ и БК вычисляются на основе секретного базового мастер-ключа ДЦ $MK_{ДЦ}$. Этот ключ генерируется ЦУК при инициализации ДЦ и передается в ДЦ. ЦУК хранит все мастер-ключи $MK_{ДЦ}$, обеспечивая их восстановление, а также смену после истечения срока эксплуатации или при экстренной необходимости.

Для каждой пары БК и ДЦ следующим образом вычисляется ключ парной связи $K_{ДЦ,БК}$:

$$K_{ДЦ,БК} = F(MK_{ДЦ}, Id_{БК} \| Id_{ДЦ}), \quad (3)$$

где F — функция вычисления производного ключа, $Id_{БК}$ и $Id_{ДЦ}$ — идентификаторы БК и ДЦ.

ДЦ может вычислять этот ключ непосредственно перед выполнением операции защиты сообщений с БК. Возможно также кэширование этих ключей. В БК ключ парной связи записывается при помощи протокола управления ключами.

Непосредственно для шифрования/расшифрования и имитозащиты сообщений между БК и ДЦ используется суточный ключ $K_{ДЦ,БК}^{d}$, вычисляемый следующим образом:

$$K_{ДЦ,БК}^{d} = F(K_{ДЦ,БК}, d), \quad (4)$$

где d — дата передачи сообщения (рассматривается как строка битов).

На рис. 2 приведена схема зависимости ключей шифрования.

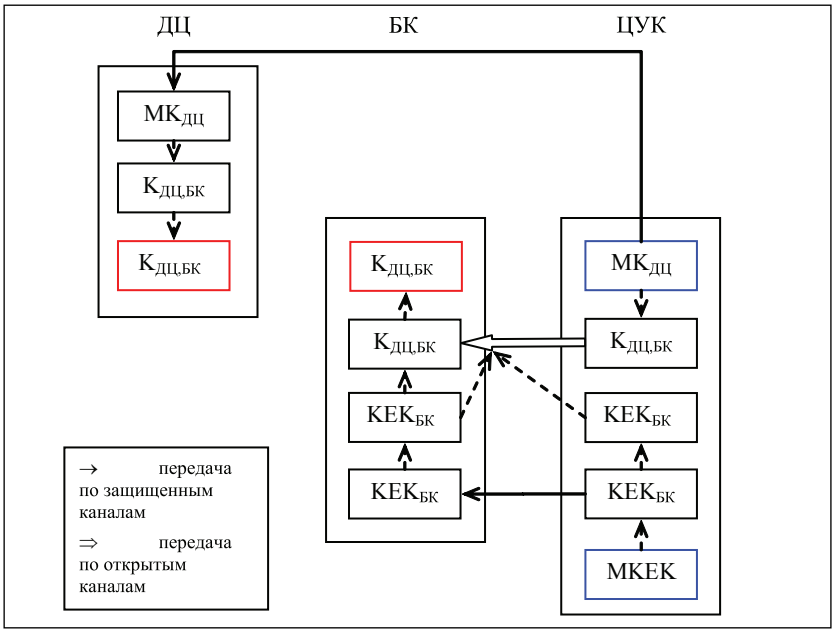

Рис. 2. Структура ключевой системы шифрования

4. Ключи цифровой подписи сообщений

Для вычисления цифровой подписи сообщений от БК в ДЦ используется следующая КИ:

- $SK_{БК}$: закрытый ключ вычисления цифровой подписи БК; генерируется БК при смене ключей; присутствует только в БК;
- $РК_{БК}$: открытый ключ проверки цифровой подписи БК; вычисляется БК при смене ключей; передается на ЦУК в ходе протокола смены ключей и далее на все ДЦ и ЦО в составе сертификата открытого ключа БК;
- $СРК_{БК}$: сертификат открытого ключа цифровой подписи БК; вычисляется ЦУК в ходе протокола смены ключей; рассылается в ДЦ и ЦО, связанные с БК.

5. Ключи цифровой подписи сертификатов

Для вычисления/проверки цифровой подписи ЦУК под сертификатами открытых ключей БК используются следующие ключи:

- KSK: закрытый ключ вычисления цифровой подписи сертификатов открытых ключей; генерируется с помощью физического ДСЧ при инициализации ЦУК; присутствует только в ЦУК;
- КРК: открытый ключ проверки цифровой подписи сертификатов открытых ключей ЦУК; вычисляется ЦУК при его инициализации;
- СКРК: сертификат открытого ключа цифровой подписи ЦУК; самоподписанный сертификат, используемый для проверки подписей под сертификатами открытых ключей БК; необходим для доставки КРК в ЦО и ДЦ.

6. Функция вычисления производных ключей

Для вычисления производного ключа предлагается использовать следующую функцию [4]:

$$F(MK, X) = H(MK||X),$$

где МК — мастер-ключ, X — дополнительная информация, H — криптографическая хэш-функция без ключа; значение H вычисляется по алгоритмам ГОСТ Р 34.11.

7. Защита сообщений от БК к ДЦ

Сообщения от БК к ДЦ передаются в подписанной и зашифрованной форме. Обратно — в зашифрованном виде с имитозащитой. Тем самым обеспечивается их конфиденциальность, целостность и аутентификация.

Формат подписанного и зашифрованного сообщения от БК к ДЦ приведен на рис. 3.

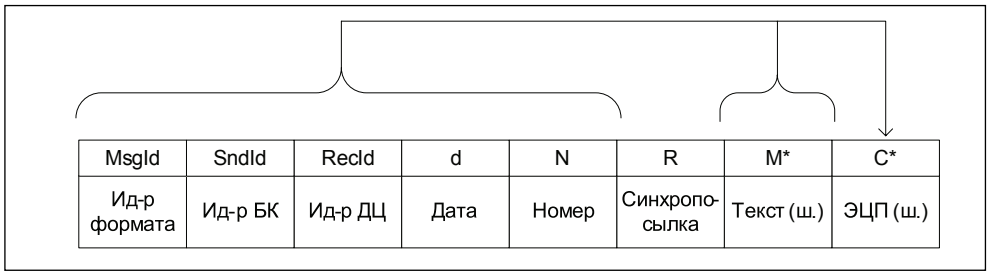

Рис. 3. Формат зашифрованного и подписанного сообщения от БК к ДЦ

После расшифрования сообщения в ДЦ оно вместе со значением цифровой подписи передается на обработку в ЦО в формате, который приведен на рис. 4.

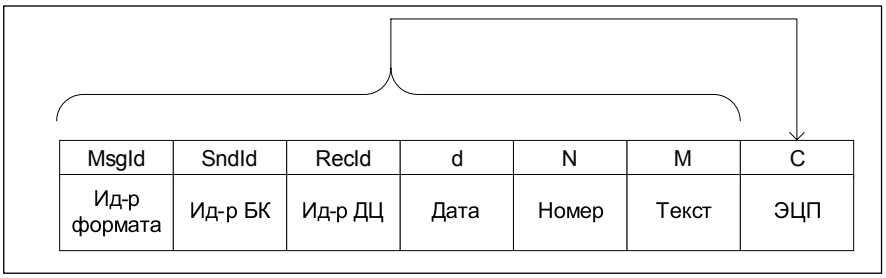

Рис. 4. Формат подписанного сообщения от БК к ДЦ в ЦО

Здесь использованы следующие обозначения:

- MsgId — идентификатор формата сообщения, константа;
- SndId — идентификатор отправителя;
- RecId — идентификатор получателя;
- d — дата отправки сообщения;
- N — номер сообщения в день d;
- R — синхропосылка шифрования;
- M — текст передаваемого сообщения;
- M* — зашифрованное сообщение M;
- C — значение цифровой подписи;
- C* — зашифрованное значение цифровой подписи.

Шифрование/расшифрование выполняется в режиме гаммирования с обратной связью по ГОСТ 28147 на ключе $K_{ДЦ,БК}^{d}$ с использованием синхропосылки R по формулам (5) и (6).

$$(M^*\|C^*) = E(K_{ДЦ,БК}^{d}, R, M\|C), \quad (5)$$

$$(M\|C) = D(K_{ДЦ,БК}^{d}, R, M^*\|C^*), \quad (6)$$

где E обозначает преобразование шифрования, D — расшифрования.

ЭЦП сообщения M вычисляется на закрытом ключе подписи БК ($SK_{БК}$) по формуле (7):

$$C = S(SK_{БК}, MsgId\|SndId\|RecId\|d\|N\|M), \quad (7)$$

где S обозначает функцию вычисления ЭЦП.

8. Защита сообщений от ДЦ к БК

Шифрование/расшифрование выполняется по формулам (5) и (6). Имитовставка вычисляется на ключе $K_{ДЦ,БК}^{d}$ по формуле (8):

$$C = I(K_{ДЦ,БК}^{d}, M), \quad (8)$$

где I обозначает функцию вычисления имитовставки по ГОСТ 28147.

Сообщения от ДЦ к БК передаются в формате, приведенном на рис. 5.

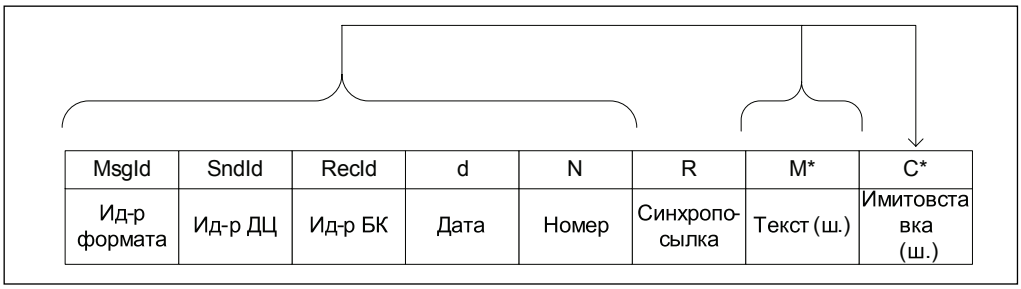

Рис. 5. Формат зашифрованного сообщения от ДЦ к БК

Сходным образом выполняется криптографическая защита управления ключами между ЦУК и БК. При этом используются ключи управления ключами $КЕК_{БК}^{d}$.

Протоколы обмена защищенными сообщениями между БК и ДЦ, а также протоколы управления ключами между ЦУК и БК построены на базе классических протоколов «рукопожатия» [5] с использованием даты/счетчика и нонсов.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
2. ГОСТ Р 34.10–2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
3. ГОСТ Р 34.11–94. Информационная технология. Криптографическая защита информации. Функция хэширования.
4. ISO/IEC 11770–2:2008. Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques.
5. ISO/IEC 9798–4:1999. Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function.