Федеральное государственное унитарное предприятие
«НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР «АТЛАС»

название изделия

Средство криптографической защиты информации (СКЗИ) Микрик

назначение, область применения

В развитие разработок российских интеллектуальных карт РИК-1 и РИК-2 ФГУП «НТЦ «Атлас» разработано средство криптографической защиты информации Микрик (далее – СКЗИ Микрик). СКЗИ Микрик реализовано на базе микроконтроллера серии MIK51 (производитель ПАО «Микрон») и совместимо с РИК-1 и РИК-2.

В настоящее время СКЗИ Микрик изготавливается в виде пластиковой карты, также возможно его изготовление в виде USB-токена.

СКЗИ Микрик предназначено для использования в следующих сферах:

- информационные системы, требующие надёжной аутентификации пользователей;
- в качестве СКЗИ или носителя ключевой и идентификационной информации в защищенных информационных системах;
- хранения персональных данных;
- в качестве модуля безопасности различного оборудования.

функции изделия

СКЗИ Микрик обеспечивает выполнение следующих функций:

- односторонняя и взаимная аутентификация СКЗИ и терминального оборудования на основе симметричной криптографии;
- вычисление парного ключа на основе алгоритма согласования ключе VKO с использованием ГОСТ 34.10-2012 (Рекомендации ТК26);
- идентификация владельца СКЗИ на основе пароля;
- шифрование/расшифрование данных;
- выработка имитовставки;
- диверсификация ключей;
- вычисление функции хэширования сообщения;
- вычисление электронной подписи;
- проверка электронной подписи;
- генерация пары: ключ подписи/ключ проверки подписи;
- структурированный доступ к информации, хранящейся в энергонезависимой памяти СКЗИ с гибкой системой разграничения доступа;
- возможность криптографической защищенности обмена информацией между картой и терминальным оборудованием.

СКЗИ Микрик поддерживает систему расширения функциональности, реализованную путем загрузки и исполнения специализированных функциональных модулей, что существенно расширяет возможности его использования без снижения уровня безопасности.

основные технические характеристики изделия

Технические и алгоритмические параметры СКЗИ Микрик соответствует стандартам:

- ГОСТ Р ИСО/МЭК 7816-3-2013;
- ГОСТ Р ИСО/МЭК 7816-4-2013.

В СКЗИ Микрик реализованы следующие алгоритмы криптографических преобразований:

- ГОСТ 28147-89;
- ГОСТ Р 34.10-2001;
- ГОСТ Р 34.10-2012;
- ГОСТ Р 34.11-94;
- ГОСТ Р 34.11-2012;
- и криптографические протоколы на их основе.

В зависимости от исполнения СКЗИ Микрик имеет класс защиты КС3 или КВ1.
СКЗИ Микрик обладает средствами защиты от сбоев и нештатных ситуаций. При каждом включении карты проводится тестирование узлов микроконтроллера.

ХАРАКТЕРИСТИКИ ОПЕРАЦИОННОЙ СИСТЕМЫ	ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ МИКРОКОНТРОЛЛЕРА
· Соответствие стандартам ISO/IEC 7816; · Реализованы современные российские криптографические алгоритмы и протоколы, включая, ГОСТ 28147-89, ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012; · Гибкая система разграничения доступа · Встроенная система загрузки и исполнения специализированных функциональных модулей; · Внутреннее самотестирование; · Система защиты от сбоев.	**Микропроцессор:** · семейство MIK51; · 8 разрядное ядро, до 33 МГц; · сопроцессоры ГОСТ 28147-89, ГОСТ Р 34.10-2012; · аппаратный ГСЧ; · модуль вычисления CRC; · ОЗУ: 6 Кбайт; · аппаратная система безопасности. **ЭСППЗУ(EEPROM):** · 72 Кбайт; · 100 000 циклов стирания/записи; · 10 лет хранения записанной информации. **Программная память (ROM):** · 160 КБайт **Диапазон рабочих температур:** · от минус 30 °С до плюс 80 °С

контакты
127018, г. Москва, ул. Образцова, 38
телефон: (495) 689-14-64
e-mail: info@stcnet.ru
http://web.stcnet.ru