

УТВЕРЖДЕНО
ИПФШ.467444.006ПП-ЛУ

**ПРОГРАММНО-АППАРАТНОЕ ШИФРОВАЛЬНОЕ (КРИПТОГРАФИЧЕСКОЕ)
СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ «КАРТА ТАХОГРАФА «ДИАМАНТ-2»**

Правила пользования

ИПФШ.467444.006ПП

Содержание

1. Общие положения	3
2. Основные функции и характеристики СКЗИ	5
3. Занесение ключевой информации в СКЗИ	8
4. Учет и хранение СКЗИ при изготовлении и эксплуатации	8
5. Действия при компрометации ключевых документов	10
6. Срок действия СКЗИ	10
7. Меры безопасности при использовании СКЗИ	10
8. Лист регистрации изменений	11

1. Общие положения

1.1. Термины и определения

Тахограф – техническое средство контроля, обеспечивающее непрерывную, некорректируемую регистрацию информации о скорости и маршруте движения транспортного средства, о режиме труда и отдыха водителей транспортного средства.

Блок СКЗИ тахографа – программно-аппаратное шифровальное (криптографическое) средство защиты информации, реализующее алгоритмы криптографического преобразования информации и обеспечивающее:

- аутентификацию;
- регистрацию информации в некорректируемом виде в защищенной памяти (далее - защищенный архив блока СКЗИ тахографа);
- хранение информации ограниченного доступа, используемой для создания электронной подписи и проверки электронной подписи (далее - ключевой информации), и аутентифицирующей информации;
- преобразование сигналов ГНСС в данные о текущем времени и о координатах местоположения транспортного средства в некорректируемом виде.

Транспортное средство (ТС) – средство автотранспорта, подлежащее, в соответствии с российским законодательством, оснащению тахографом.

Предприятия – юридические лица и индивидуальные предприниматели, осуществляющие на территории Российской Федерации деятельность, связанную с эксплуатацией транспортных средств (далее - транспортные предприятия).

Пользователи тахографа – предприятия, водители, сотрудники контрольных органов, сотрудники мастерских.

Жизненный цикл тахографа – комплекс операций и процессов, включающий разработку, производство, активизацию, настройку, эксплуатацию, ремонт, техническое обслуживание, вывод из эксплуатации тахографа.

Мастерская – юридические лица и индивидуальные предприниматели, осуществляющие работы по установке, проверке, техническому обслуживанию и ремонту устанавливаемых на транспортные средства тахографов, сведения о которых учтены ФБУ «Росавтотранс» в перечне мастерских.

Активация тахографа – внесение в блок СКЗИ тахографа с использованием карты мастерской установочных данных, включая идентификационные данные транспортного средства и квалифицированные сертификаты ключей проверки электронной подписи (далее – квалифицированный сертификат) блока СКЗИ тахографа.

Активация тахографа выполняется:

- при установке нового тахографа на транспортное средство;
- при переносе тахографа с одного транспортного средства на другое;
- при ремонте тахографа, с заменой блока СКЗИ тахографа (поломка или окончание срока эксплуатации).

Настройка тахографа – процедура обновления или подтверждения параметров транспортного средства, которые должны храниться в памяти блока СКЗИ тахографа.

СКЗИ карта тахографа «Диамант-2» – программно-аппаратное шифровальное (криптографическое) средство защиты информации «Карта тахографа «Диамант-2».

Перечень моделей карт тахографа – перечень сведений о моделях карт, формируемый в соответствии с требованиями Правил использования тахографов, установленных на транспортные средства (приложение № 3 к приказу Минтранса России от 13 февраля 2013 г. № 36).

1.2. Список сокращений и обозначений

АС – автоматизированная система.

БУ – бортовое устройство.

СКЗИ – средство криптографической защиты информации.

ТС – транспортное средство.

1.3. Назначение СКЗИ карта тахографа «Диамант-2»

Средство криптографической защиты информации «Карта тахографа «Диамант-2» разработано в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66 (зарегистрирован Минюстом России 3 марта 2005 г., регистрационный № 6382).

СКЗИ представляет собой микропроцессорную пластиковую карту с нанесенной на ее поверхность защитной графикой и текстовой информацией о владельце (пользователе) карты.

СКЗИ являются программно-аппаратным шифровальным (криптографическим) средствами защиты информации и состоят из 4-х типов карт:

- карта водителя;
- карта контролера;
- карта мастерской;
- карта предприятия.

СКЗИ имеет состоящий из четырех цифр персональный идентификационный номер (ПИН), используемый для аутентификации карты.

СКЗИ обеспечивает:

- идентификацию и аутентификацию владельца карты;
- определяют полномочия доступа владельца карт;
- конфиденциальность и целостность информации при обмене с тахографом.

2. Основные функции и характеристики СКЗИ

2.1. Карта водителя

Карта водителя обеспечивает хранение следующих идентификационных данных:

- серийный номер встроенного микропроцессора;
- учетный номер карты (СКЗИ);
- номер карты;
- наименование и адрес организации - изготовителя карты.
- наименование и адрес организации, выдавшей карту, дата выдачи;
- дата начала действия карты, дата окончания срока действия карты;
- фамилия и имя держателя карты;
- дата рождения держателя карты;
- номер водительского удостоверения;
- наименование органа, выдавшего водительское удостоверение.

Карта водителя обеспечивает:

- аутентификацию субъекта, осуществляющего доступ к функциям тахографа;

- предоставление доступа к данным карты по чтению и записи в соответствии с установленными условиями доступа;
- вычисление электронной подписи данных, хранящихся на карте;
- проверку электронной подписи;
- хранение записей данных:
 - использования транспортного средства;
 - показаний счетчика пробега транспортного средства;
- внесенных вручную водителем данных о его деятельности:
 - о координатах местоположения транспортного средства, в которых начинаются и заканчиваются ежедневные периоды работы;
 - о типах событий, зарегистрированных тахографом с введенной в него картой;
 - о видах неисправностей, обнаруженных тахографом с введенной в него картой;
 - о проверочных операциях.

2.2. Карта контролера

Карта контролера обеспечивает хранение записей следующих идентификационных данных:

- номер карты;
- название выдавшей карту организации, дата ее выдачи;
- сроки действия карты;
- название контрольного органа;
- адрес контрольного органа.

Карта контролера обеспечивает:

- аутентификацию субъекта, осуществляющего доступ к функциям тахографа;
- предоставление доступа к данным карты по чтению и записи в соответствии с установленными условиями доступа;
- вычисление электронной подписи данных, хранящихся на карте;
- проверку электронной подписи;
- хранение записей данных о проверочных операциях:
 - дата и время проверки;
 - тип проверки (вывод на дисплей и/или на печать, и/или загрузка данных с бортового устройства, и/или загрузка с карты);
 - период, за который загружаются данные (в соответствующих случаях);

- регистрационный номер транспортного средства;
- номер проверенной карты водителя и наименование организации, выдавшей карту.

2.3. Карта мастерской

Карта мастерской обеспечивает хранение данных, необходимых для осуществления активизации тахографа и блока СКЗИ тахографа.

Карта мастерской обеспечивает хранение записей следующих данных:

- серийный номер встроенного микропроцессора;
- учетный номер карты (СКЗИ);
- номер карты;
- наименование и адрес организации - изготовителя карты.
- наименование и адрес организации, выдавшей карту, дата выдачи;
- сроки действия карты;
- наименование и адрес мастерской;
- фамилия и имя держателя;
- записей данных о транспортных средствах;
- данных о периодах работы;
- данных о событиях и неисправностях;
- данных о проверочных операциях.

Карта мастерской обеспечивает:

- аутентификацию субъекта, осуществляющего доступ к функциям тахографа;
- предоставление доступа к данным карты по чтению и записи в соответствии с установленными условиями доступа;
- вычисление электронной подписи данных, хранящихся на карте;
- проверку электронной подписи;
- установку настроечных параметров тахографа и активацию блока СКЗИ тахографа;
- хранение записей о корректировках установочных данных:
 - идентификационные данные транспортного средства;
 - данные о регулировке: устройства ограничения скорости, показаний счетчика пробега (новые и прежние показания), даты и времени (новые и прежние показания);
 - хранение идентификационных данных тахографа.

2.4. Карта предприятия

Карта предприятия обеспечивает хранение следующих идентификационных данных:

- серийный номер встроенного микропроцессора;
- учетный номер карты (СКЗИ);
- номер карты;
- наименование и адрес организации - изготовителя карты.
- наименование и адрес организации, выдавшей карту, дата выдачи;
- дата начала действия карты, дата окончания срока действия карты;
- название транспортного предприятия;
- адрес транспортного предприятия.

Карта предприятия обеспечивает:

- аутентификацию субъекта, осуществляющего доступ к функциям тахографа;

- предоставление доступа к данным карты по чтению и записи в соответствии с установленными условиями доступа;

- вычисление электронной подписи данных, хранящихся на карте;

- проверку электронной подписи;

- установку настроечных параметров тахографа и активацию блока СКЗИ тахографа;

- хранение записей данных о действиях транспортного предприятия:

- дата и время осуществленного действия;

- тип действия (блокировка и/или разблокировка бортового устройства, и/или загрузка данных с тахографа, и/или загрузка данных с карты);

- период, за который загружаются данные (в соответствующем случае).

3. Занесение ключевой информации в СКЗИ

Занесение ключевой информации производится на этапе изготовления карты.

Значения параметров криптографических алгоритмов и ключевая информация загружаются в карту с использованием сертифицированных программно-аппаратных средств, организацией, обладающей соответствующей лицензией ФСБ России.

4. Учет и хранение СКЗИ при изготовлении и эксплуатации

4.1 В соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66 (зарегистрирован Минюстом России 3 марта 2005 г., регистрационный № 6382) организация поэкземплярного учёта изготавливаемых карт возлагается на организацию-изготовитель, организация поэкземплярного учёта используемых (эксплуатируемых) карт возлагается на организацию, являющуюся заказчиком карт.

4.2 Типовая форма журнала поэкземплярного учёта СКЗИ приведена в Приложении 2 к Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утверждённой Приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152.

4.3 Организация-изготовитель обеспечивают ежегодную отчетность по поэкземплярному учету карт перед ФСБ России.

4.4 При изготовлении карт поэкземплярный учёт должен производиться в следующем порядке:

4.4.1 В процессе загрузки штатного программного обеспечения каждому экземпляру карты присваивается уникальный номер карты в соответствии с установленными правилами, а также регистрационный номер поэкземплярного учета карт, выбираемый последовательно из диапазона регистрационных номеров, определенного для карт ФСБ России.

4.4.2 Номер карты наносится на каждую карту.

4.4.3 Регистрационный номер поэкземплярного учета карт записывается на электронный чип каждой карты.

4.4.4 Поэкземплярный учёт карт осуществляется по таблицам соответствия номеров карты и регистрационных номеров поэкземплярного учета изготовленных карт.

4.5 Хранение карт осуществляется в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение (порчу).

4.6 Складские помещения для хранения карт должны быть обеспечены следующими мерами защиты:

- защитой от проникновения (усиленная дверь, решётки на окнах);
- системой защиты от несанкционированного доступа с двумя независимыми контурами защиты (механический + цифровой или биометрический замок, система охранной сигнализации, видеонаблюдения);
- списком лиц, имеющих допуск в помещение и журналом выдачи ключей.

4.7 При получении соответствующих карт, пользователь получает в запечатанном конверте персональный идентификационный номер (ПИН-код и ПУК-код), представляющий собой средство защиты карт от несанкционированного использования. ПИН-код и ПУК-код удостоверяют полномочия пользователя карты на совершение операций с её использованием. Допускается наличие в запечатанном конверте дополнительных вложений.

4.8 Использование карты осуществляется в соответствии с Руководством пользователя на тахограф.

4.9 Для сохранения работоспособности карты необходимо соблюдать условия хранения карты, при этом не допускать:

- воздействия на карту источников сильного электромагнитного излучения (нахождения карты рядом с сотовым телефоном; мобильной радиостанцией и т.п.);
- механического повреждения карты;
- загрязнения карты;
- непосредственного воздействия на карту влаги, высоких температур (выше 85 °С), а также агрессивных сред, разрушающих пластик карты;

- приложения усилий при вводе карты в считыватель тахографа, а также при изъятии карты.

4.10 Замена карты с неоконченным сроком действия производится в случаях:

- наличия дефекта карты, делающего ее использование невозможным;
- работы карты со сбоями;
- порчи карты;
- утери или кражи карты;
- изменения персональных (и/или иных) данных пользователя карты.

4.11 Организация-изготовитель в течение срока действия карты может приостановить действие карты или аннулировать ее при выявлении случаев:

- подделки карты;

- использования карты лицами, не имеющими законных оснований для ее использования;
- передачи карты ее пользователем другим лицам;
- получения карты на основе ложных заявлений и/или фальшивых документов.

4.12 Приостановление действия карты и (или) аннулирование ее оформляется организацией-изготовителем в виде соответствующего решения, с указанием причин приостановления действия карты и (или) ее аннулирования.

5. Действия при компрометации ключевых документов

При выявлении события компрометации ключевого материала карта подлежит немедленной замене в установленном порядке.

6. Срок действия СКЗИ

Срок действия СКЗИ:

- 1) срок действия карт водителей не превышает трех лет;
- 2) срок действия карт контролера не превышает двух лет;
- 3) срок действия карт мастерских не превышает одного года;
- 4) срок действия карт предприятия не превышает трех лет.

7. Меры безопасности при использовании СКЗИ

Для предотвращения несанкционированного использования пользователю карты необходимо предпринимать все возможные меры для предотвращения утраты, хищения карты или незаконного ее использования, а именно:

- не передавать карту и ПИН-код другим лицам. Картой имеет право пользоваться только держатель карты;
- не записывать ПИН-код на карте;
- не хранить ПИН-код вместе с картой и не сообщать его другим лицам;
- не оставлять карту без контроля владельца;
- хранить карту в месте, недоступном для других.

В случае, если карта потеряна или украдена, владелец карты должен сообщить об этом в ФБУ «Росавтотранс».