ПРОГРАММНО-АППАРАТНОЕ ШИФРОВАЛЬНОЕ (КРИПТОГРАФИЧЕСКОЕ) СРЕДСТВО БЛОК СКЗИ ТАХОГРАФА «Навигационно-криптографический модуль «НКМ-К»

Правила пользования

ИПФШ.467756.004ПП

Содержание

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 (СКЗИ), реализующее алгоритмы криптографического преобразования информации и обеспечивающее:

- аутентификацию;
- регистрацию информации в некорректируемом виде в защищённой памяти (далее – защищённый 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.

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

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

Жизненный цикл тахографа – комплекс операций и процессов, включающий разработку, производство, активизацию, калибровку,

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.

Активизация 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.

Активизация 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).

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

Ремонт и техническое обслуживание тахографа – операции по диагностике технического состояния тахографа и замене его компонентов.

Программно-аппаратное шифровальное (криптографическое) средство защиты информации «Карта тахографа «Диамант» (далее – карты тахографа).

Карты тахографа включают в себя следующие типы карт:

- **карта водителя** - обеспечивает идентификацию и аутентификацию водителя с использованием шифровальных (криптографических) средств, а также хранение данных о деятельности водителя;
- **карта контролера** - обеспечивает идентификацию и аутентификацию контрольного органа и соответствующего сотрудника контрольного

органа (владельца карты) с использованием шифровальных (криптографических) средств;

- **карта мастерской** - обеспечивает идентификацию и аутентификацию держателя карты с использованием шифровальных (криптографических) средств;
- **карта предприятия** - обеспечивает идентификацию и аутентификацию транспортных предприятий, с использованием шифровальных (криптографических) средств, установку блокировки (ограничения) доступа к данным тахографа и данным карт водителей.

Перечень [карт тахографа, тахографов, блоков СКЗИ тахографа] – перечни сведений, формируемых в соответствии с требованиями Правил использования тахографов, установленных на транспортные средства (приложение № 3 к приказу Минтранса России от 13 февраля 2013 г. № 36).

Криптографический ключ (криптоключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе (далее – ключ).

Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

1.2 Список сокращений и обозначений

АС – автоматизированная система.

БУ – бортовое устройство.

ГНСС – глобальная навигационная спутниковая система.

СКЗИ – средство криптографической защиты информации.

ТС – транспортное средство.

НКМ-К – Программно-аппаратное шифровальное (криптографическое) средство блок СКЗИ тахографа «Навигационно-криптографический модуль НКМ-К».

УЦ – Удостоверяющий центр.

1.3 Назначение НКМ-К

Программно-аппаратное шифровальное (криптографическое) средство блок СКЗИ тахографа «Навигационно-криптографический модуль «НКМ-К» (далее – НКМ-К) является компонентом тахографа, предназначенным для реализации криптографических алгоритмов, необходимых для вычисления квалифицированной электронной подписи, проведения процедур аутентификации и обеспечения защиты информации, обрабатываемой и хранимой в тахографе и подлежащей защите в соответствии с законодательством Российской Федерации.

НКМ-К представляет собой средство защиты информации, класса КС3 и способен противостоять соответствующим атакам.

1.4 Перечень документов, на основании которых осуществляется разработка и эксплуатация НКМ-К

– Кодекс Российской Федерации об административных правонарушениях.

– Федеральный закон от 10 декабря 1995 г. № 196-ФЗ «О безопасности дорожного движения».

– Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

– Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

– Федеральный закон от 03 апреля 1995 г. № 40-ФЗ «О Федеральной службе безопасности».

– Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

– Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

– Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

– Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

– Постановление Правительства Российской Федерации от 06 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

– Постановление Правительства Российской Федерации от 09 февраля 2012 г. № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи».

– Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

– Приказ ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

– Приказ ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

– Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении 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».

– Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утверждены ФСБ России от 21 февраля 2008 г. № 149/6/6-622.

– Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утверждены ФСБ России 21 февраля 2008 г. № 149/54-144.

– Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального

предпринимателя), утвержденное постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313.

– Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ 2005), утверждённое приказом ФСБ России от 9 февраля 2005 г. № 66.

– Требования к средствам электронной подписи и требования к средствам удостоверяющего центра, утверждённые приказом ФСБ России от 27 декабря 2011 г. № 796.

– Требования к тахографам, устанавливаемым на транспортные средства, утверждённые приказом Министерства транспорта Российской Федерации от 13 февраля 2013 г. № 36.

– Правила использования тахографов, установленных на транспортные средства утверждённые приказом Министерства транспорта Российской Федерации от 13 февраля 2013 г. № 36.

– Правила обслуживания тахографов, установленных на транспортные средства утверждённые приказом Министерства транспорта Российской Федерации от 13 февраля 2013 г. № 36.

– Правила контроля работы тахографов, установленных на транспортные средства утверждённые приказом Министерства транспорта Российской Федерации от 13 февраля 2013 г. № 36.

– ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

– ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хеширования.

– ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

– ГОСТ Р ИСО/МЭК 7816-4-2004 Информационная технология. Карты идентификационные. Карты на интегральных схемах с контактами. Часть 4. Межотраслевые команды для обмена.

2 Основные технические характеристики НКМ-К

2.1 Состав НКМ-К

В комплект поставки НКМ-К входят:

- НКМ-К;
- Формуляр.

2.2 Технические характеристики НКМ-К

НКМ-К должно монтироваться на плату внутри корпуса бортового устройства тахографа.

Подключение НКМ-К к плате тахографа осуществляется через разъём FCI 87409-110, 20.

Подключение кабеля антенны приёмника ГЛОНАСС осуществляется через разъём - MMCX (Amphenol 908-24100).

Питание НКМ-К осуществляется от источника питания тахографа.

Напряжение питания постоянное 3,3 В ± 5 %, 5,0 В ± 5 % с заземлённым «минусом».

2.3 Функции НКМ-К и поддерживаемые криптографические алгоритмы

НКМ-К в составе тахографа выполняет следующие функции:

- проведение взаимной аутентификации карт тахографа и НКМ-К;
- формирование и передача в процессор тахографа данных о параметрах движения транспортных средств на основании данных ГНСС (текущая скорость, координаты);
- формирование и передача в процессор тахографа данных о текущем времени в формате UTC (SU);
- архивирование данных о координатах, скорости транспортного средства и текущем времени в формате UTC (SU);
- архивирование данных о событиях НКМ-К;
- архивирование данных о событиях тахографа;

- архивирование данных по запросу от тахографа;

- обеспечение хранения данных в некорректируемом виде в архиве НКМ-К;
- долговременное хранение зарегистрированных данных (за последние 365 дней) в некорректируемом виде в архиве НКМ-К, в том числе, идентификационных данных, вводимых в НКМ-К;
- обеспечение конфиденциальности, целостности и аутентификации данных, загружаемых из архива НКМ-К на внешние носители информации;
- управление разграничением доступа к данным архива НКМ-К;
- обеспечение конфиденциальности, целостности и аутентификации данных, передаваемых между тахографом и картами тахографа;
- хранение ключевой информации.

НКМ-К обеспечивает выполнение следующих криптографических алгоритмов:

- шифрование и расшифрование данных по алгоритму ГОСТ 28147-89 в режиме простой замены;
- шифрование и расшифрование данных по алгоритму ГОСТ 28147-89 в режиме простой замены с зацеплением;
- вычисление криптографической контрольной суммы по алгоритму ГОСТ 28147-89 в режиме выработки имитовставки;
- вычисление значения хэш-функции заданного сообщения по алгоритму ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012;
- вычисление значения электронной цифровой подписи с использованием алгоритма ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012;
- проверку значения электронной цифровой подписи, сформированной с использованием алгоритма ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012;
- согласование ключей в соответствии с алгоритмом «VKO GOST R 34.10-2001».

3 Ключевая система НКМ-К и ключевые носители

3.1 Состав ключей НКМ-К

Обозначение	Определение	Срок действия ключей НКМ-К
Sкс	Закрытый ключ тахографа	3 года
Ркс	Открытый ключ проверки электронной подписи тахографа	6 лет
$P_{CA}n$	Открытый ключ проверки электронной подписи УЦ для проверки сертификата устройства	15 лет

3.2 Занесение ключевой информации в энергонезависимую память

Занесение ключевой информации в НКМ-К производится на этапе производства НКМ-К.

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

Загрузка сертификатов открытых ключей НКМ-К осуществляется в процессе проведения активизации НКМ-К в составе тахографа.

4 Учёт и хранение НКМ-К и криптографических ключей

4.1 Учёт и хранение НКМ-К

4.1.1 Учёт и хранение НКМ-К при распространении

Организация поэкземплярного учёта НКМ-К возлагается на предприятие-заказчика.

При хранении НКМ-К в организации, осуществляющей распространение НКМ-К, поэкземплярный учёт и хранение НКМ-К должны производиться в следующем порядке:

1) Поэкземплярный учёт НКМ-К осуществляет уполномоченный сотрудник организации, внесением соответствующих записей в журнал учёта НКМ-К.

2) При распространении НКМ-К должна производиться проверка наличия у покупателя НКМ-К лицензий ФСБ России на деятельности по распространению шифровальных (криптографических) средств.

3) При передаче НКМ-К производитель должен записывать реквизиты покупателя в журнале поэкземплярного учёта НКМ-К.

4) Распространитель НКМ-К должен вести журнал поэкземплярного учёта НКМ-К с указанием: даты приобретения НКМ-К, даты продажи НКМ-К, реквизитов покупателей НКМ-К.

5) Складские помещения распространителя НКМ-К должны быть обеспечены следующими мерами защиты:

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

4.1.2 Учёт и хранение НКМ-К при встраивании их в тахограф

При проведении работ по встраиванию НКМ-К в тахограф поэкземплярный учёт НКМ-К должен производиться в следующем порядке:

1) Организация, осуществляющая встраивание НКМ-К в тахограф должна обеспечить учёт приобретенных НКМ-К в журнале поэкземплярного учёта НКМ-К. В журнале поэкземплярного учёта НКМ-К регистрируются заводские номера тахографов, в которые устанавливаются НКМ-К.

2) Данные об заводских и регистрационных номерах НКМ-К и заводских номерах тахографов, в которые НКМ-К были встроены, по защищённому каналу, обеспечивающему целостность и конфиденциальность передаваемой информации, направляются в ФБУ «Росавтотранс» для включения в соответствующий перечень.

3) Оборудование складских помещений организации, выполняющей работы по встраиванию НКМ-К в тахограф, должно обеспечивать:

- защиту от проникновения (усиленная дверь, решетки на окнах);
- защиту от несанкционированного доступа, состоящую из двух независимых контуров защиты (механический + цифровой или биометрический замок, система охранной сигнализации, видеонаблюдения);
- учёт лиц, имеющих допуск в помещение и журнал выдачи ключей.

4) При поставках тахографов со встроенными НКМ-К производитель тахографа должен производить запись реквизитов покупателя (распространителя) тахографа в журнале поэкземплярного учёта НКМ-К.

4.1.3 Учёт НКМ-К при распространении и эксплуатации в составе тахографа

Учёт НКМ-К в соответствующих перечнях ведется ФБУ «Росавтотранс» в соответствии с требованиями приказа Минтранса России от 13 февраля 2013 г. № 36.

Владельцы транспортных средств ведут учёт тахографов с встроенными НКМ-К в рамках установленных правил учёта материальных ценностей.

4.1.4 Учёт и хранение НКМ-К при техническом обслуживании тахографов

Мастерские, приобретая НКМ-К, должны обеспечить их поэкземплярный учёт, записывая в журнал поэкземплярного учета НКМ-К учётные номера НКМ-К.

Хранение НКМ-К должно осуществляться на складе Мастерской, оборудование которого обеспечивает:

- защиту от проникновения (усиленная дверь, решетки на окнах);
- защиту от несанкционированного доступа, содержащую два независимых контура защиты (механический + цифровой или биометрический замок, система охранной сигнализации, видеонаблюдения);
- учёт лиц, имеющих допуск в помещение и журнал выдачи ключей.

При активизации тахографа представитель Мастерской должен провести следующие учётные операции:

- сделать запись в журнале поэкземплярного учёта НКМ-К о заводском и регистрационном номерах НКМ-К, установленного на заданное транспортное средство и внести в журнал запись о реквизитах владельца транспортного средства;
- по защищённому каналу, обеспечивающему целостность и конфиденциальность передаваемой информации, используя карту мастерской передать в ФБУ «Росавтотранс» данные:
    - о заводском и регистрационном номерах НКМ-К;
    - об активизации тахографа и его заводской номер.

При замене отработавшего срок эксплуатации или отказавшего НКМ-К представитель Мастерской должен провести следующие учётные операции:

- сделать запись в журнале поэкземплярного учёта НКМ-К об установке НКМ-К с данным заводским и регистрационным номерами в тахограф, установлённый на конкретное транспортное средство, и внести в журнал запись о транспортном средстве и его владельце;

- по защищённому каналу, обеспечивающему целостность и конфиденциальность передаваемой информации, направить в ФБУ «Росавтотранс» данные:
    - о заводском и регистрационном номерах снятого с тахографа НКМ-К, для установки его статуса в состояние «заблокирован»;
    - о заводском и регистрационном номерах НКМ-К, установленного взамен снятого, для установки его статуса в состояние «ТС активировано»;
    - о заводском номере тахографа, в котором заменён НКМ-К.

4.2 Учёт и хранение криптографических ключей

4.2.1 Порядок учёта и хранения криптографических ключей НКМ-К

Учёт криптографических ключей НКМ-К ведётся в составе мер учёта НКМ-К в соответствии с порядком, установленным в разделе «Учёт и хранение НКМ-К». Отдельные операции учёта ключевых документов не организуются.

Срок действия ключевых документов НКМ-К составляет три года с момента активизации НКМ-К.

Эксплуатация НКМ-К с истекшим сроком действия ключевой информации запрещается. НКМ-К с истекшим сроком действия ключевой информации подлежит замене. Тахограф за 60 дней до истечения срока действия ключевой информации НКМ-К, формирует сообщение о дате истечения срока действия ключевой информации НКМ-К и о необходимости замены НКМ-К.

4.2.2 Порядок работы с ключами при техническом обслуживании и утилизации НКМ-К

1. При замене отработавшего срок эксплуатации НКМ-К организация, имеющая лицензию ФСБ России на выполнение работ и оказание услуг по пунктам 12 или 20 Перечня выполняемых работ в соответствии с Приложением к постановлению Правительства Российской Федерации от 16 апреля 2012 г. № 313, должна, во избежание несанкционированного использования НКМ-К, используя сертифицированные ФСБ России средства, уничтожить ключевую информацию, содержащуюся в НКМ-К. При этом сертификат открытого ключа НКМ-К должен быть сохранен в составе НКМ-К для обеспечения возможности выгрузки данных из защищенного архива НКМ-К.

Уничтожение ключевой информации НКМ-К осуществляется в соответствии с требованиями п. 46 «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», утвержденной приказом ФАПСИ от 13 июня 2001 г. № 152.

Информация о выводе НКМ-К из эксплуатации и об уничтожении ключевой информации в НКМ-К (заводской номер и дата уничтожения ключевой информации) передается в ФБУ «Росавтотранс».

2. В случае отсутствия сертифицированных ФСБ средств, применяемых для уничтожения ключевой информации, содержащейся в НКМ-К, при замене отработавшего срок эксплуатации НКМ-К, организация, имеющая лицензию ФСБ России (на выполнение работ и оказание услуг по пункту 21 Перечня выполняемых работ в соответствии с Приложением к постановлению Правительства Российской Федерации от 16 апреля 2012 г. № 313), на основе договора с владельцем транспортного средства оставляет отработавшие срок эксплуатации НКМ-К для хранения.

3. После уничтожения ключевой информации, НКМ-К с сохраненным сертификатом открытого ключа должен передаваться, организацией, уничтожившей ключевую информацию, по акту владельцу транспортного средства для хранения. При этом срок хранения НКМ-К после его вывода из эксплуатации должен быть не менее года. Информация об уничтожении ключевой информации в НКМ-К (наименование изделия, дата его выпуска, заводской номер, регистрационный номер поэкземплярного учета, дата вывода из эксплуатации и дата уничтожения ключевой информации) передается в ФБУ «Росавтотранс».

4. Отработавшие срок эксплуатации НКМ-К, после хранения или НКМ-К, признанные отказавшими в процессе эксплуатации на основании заключения экспертной лаборатории, подлежат утилизации (уничтожению) путем физического уничтожения материального носителя НКМ-К, что оформляется соответствующим актом. В акте указываются: наименование изделия, дата его выпуска, заводской номер, регистрационный номер поэкземплярного учета, дата уничтожения, подписи членов комиссии по уничтожению материального носителя НКМ-К с их расшифровкой. Информация об утилизации (физическом уничтожении) материального носителя НКМ-К (заводской номер, дата уничтожения) передается в ФБУ «Росавтотранс».

5. Утилизация НКМ-К проводится путем его механического разрушения (прессование, дробление электронного модуля НКМ-К). Факт утилизации НКМ-К оформляется актом произвольной формы. Срок хранения акта определяется действующими нормативными документами.

4.2.3 Порядок действий при компрометации ключевых документов

Событием компрометации ключевой информации НКМ-К является любое нарушение целостности корпуса тахографа в процессе его эксплуатации, в результате которого могло бы произойти несанкционированное изъятие НКМ-К из защищенного корпуса тахографа.

При выявлении события компрометации ключевой информации НКМ-К подлежит немедленной замене в установленном порядке.

5 Использование НКМ-К

5.1 Порядок встраивания НКМ-К в тахограф

5.1.1 Испытания функциональности и совместимости при встраивании НКМ-К в тахограф

Для проведения оценки влияния аппаратных, аппаратно-программных и программных средств тахографа на выполнение заданных требований по безопасности информации, предъявляемых к НКМ-К при его функционировании в штатном режиме, разработчику НКМ-К должен быть представлен опытный образец модели тахографа со встроенным НКМ-К. 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 оценка влияния осуществляется разработчиком НКМ-К совместно со специализированной организацией. Результаты оценки влияния (испытаний) в форме отчета, а также образец НКМ-К и опытный образец тахографа, с которыми проводились исследования, направляются для проведения экспертизы в ФСБ России, которая готовит соответствующее заключение. При положительном заключении ФСБ России допускается совместное использование тахографа и НКМ-К.

Для испытаний функциональности и совместимости производитель тахографа должен предоставить разработчику НКМ-К:

- опытный образец тахографа со встроенным НКМ-К;
- техническую (конструкторскую и программную) документацию на тахограф, описывающую все взаимодействия тахографа с НКМ-К;
- протоколы испытаний тахографа со встроенным НКМ-К (в соответствии с техническими условиями).

Испытания функциональности и совместимости должны производиться для каждой версии программного обеспечения тахографа. При изменении версии (обновлении) программного обеспечения тахографа испытания

функциональности и совместимости должны производиться повторно в полном объёме.

Встраивание НКМ-К в тахограф должно производиться для тахографов, прошедших испытания функциональности и совместимости и получивших положительное Заключение о совместимости.

5.1.2 Технологический процесс производства тахографов со встроенным НКМ-К

Установка НКМ-К в тахограф на производственном участке должна производиться в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утверждённым приказом ФСБ России от 9 февраля 2005 г. № 66.

Контроль работоспособности НКМ-К в составе тахографа должен обеспечивать выполнение операции диагностики НКМ-К.

Производитель НКМ-К может участвовать в контроле процесса встраивания НКМ-К в тахограф в том числе осуществлять:

- согласование документов технологического процесса;
- анализ данных событийного протоколирования;
- анализ отчетности по производственным операциям, предоставляемым производителем тахографа;
- плановые и внеплановые проверки.

Производитель тахографа должен предоставить производителю НКМ-К необходимые технические и организационные условия для осуществления участия в контроле за встраиванием НКМ-К в тахограф.

Производитель НКМ-К вправе обращаться в установленном порядке по осуществлению контроля и расследования инцидентов при встраивании НКМ-К в тахограф в Управления ФСБ России.

5.2 Порядок эксплуатации НКМ-К в составе тахографа

Эксплуатация НКМ-К в составе тахографа должна выполняться в соответствии с настоящими Правилами пользования и техническими условиями на НКМ-К.

Нарушения процесса эксплуатации тахографа, приведшие к нарушению целостности защиты корпуса тахографа, должны рассматриваться, как событие компрометации НКМ-К и вести к замене НКМ-К.

5.3 Порядок технического обслуживания НКМ-К

5.3.1 Операции технического обслуживания НКМ-К

В ходе технического обслуживания НКМ-К могут выполняться следующие операции:

- диагностика НКМ-К в составе тахографа путём печати отчёта о техническом состоянии НКМ-К;
- диагностика НКМ-К в составе тахографа путём выдачи отчёта о техническом состоянии НКМ-К на карту тахографа;
- замена НКМ-К при ремонте тахографа;
- замена отработавшего срок эксплуатации или отказавшего НКМ-К;
- уничтожение секретного ключа отработавшего срок эксплуатации НКМ-К и неисправного НКМ-К.

5.3.2 Место проведения технологических операций и субъекты технического обслуживания

Активизация тахографа со встроенным НКМ-К и замена отработавшего срок эксплуатации или неисправного НКМ-К могут производиться как на территории Мастерской, так и на удаленном Посту активизации тахографа с использованием соответствующего сертифицированного оборудования.

Диагностика НКМ-К в составе тахографа может производиться любым пользователем тахографа, аутентифицированным при помощи карты тахографа (Водителя, Предприятия, Мастерской, Контролера) путём печати отчёта о техническом состоянии НКМ-К.

5.3.3 Активизация и диагностика НКМ-К

При активизации НКМ-К должно обеспечиваться выполнение следующих требований:

- НКМ-К в организации - изготовители тахографов и в мастерские поступают с загруженной ключевой информацией;
- ключевая информация, загруженная в НКМ-К в процессе его производства, до загрузки в него квалифицированного сертификата НКМ-К и завершения активизации НКМ-К не принадлежит владельцу транспортного средства;
- активизация НКМ-К осуществляется после аутентификации им карты мастерской;
- тахограф с неактивизированным НКМ-К записывает на карту мастерской данные, необходимые для создания квалифицированного сертификата ключа НКМ-К (далее - данные для создания сертификата ключа);
- мастерская направляет данные для создания сертификата ключа в аккредитованный удостоверяющий центр;
- мастерская, получив квалифицированный сертификат ключа НКМ-К, записывает его на карту мастерской;
- ввод квалифицированного сертификата ключа НКМ-К с карты мастерской в НКМ-К осуществляется путём ввода карты мастерской в тахограф, ввода PIN-кода и аутентификации карты мастерской НКМ-К;
- проверка завершения загрузки квалифицированного сертификата ключа НКМ-К с карты мастерской в НКМ-К проводится путём взаимной аутентификации карты мастерской и НКМ-К;
- после загрузки в НКМ-К квалифицированного сертификата ключа НКМ-К осуществляется загрузка в НКМ-К идентификационных данных транспортного средства, а также установочных параметров, требующих сохранения в защищённом архиве НКМ-К;

- после загрузки в НКМ-К идентификационных данных транспортного средства и установочных параметров, требующих сохранения в защищённом архиве НКМ-К, активизация НКМ-К завершается, ключевая информация, загруженная в НКМ-К, с этого момента принадлежит владельцу транспортного средства;
- мастерская направляет сведения об активизированных тахографе и НКМ-К для их внесения в соответствующие перечни.

Диагностика тахографа со встроенным НКМ-К путём печати отчёта должна выполняться в следующем порядке:

- пользователь должен аутентифицироваться при помощи карты тахографа;
- пользователь должен запросить функцию вывода данных диагностики НКМ-К на печать;
- тахограф должен сформировать отчёт, в который автоматически включается текущее время, дата, координаты местонахождения транспортного средства и заводской номер НКМ-К тахографа, подписанные квалифицированной электронной подписью;
- при выгрузке на внешние носители данных, содержащихся в памяти бортового устройства, в состав этих данных НКМ-К автоматически включается текущее время, дата, координаты местонахождения транспортного средства и заводской номер НКМ-К, подписанные квалифицированной электронной подписью;
- доступ к памяти защищённого архива НКМ-К осуществляется только после проведения взаимной аутентификации карты (контролера, мастерской, предприятия) и НКМ-К;
- данные о проведенной аутентификации карты регистрируются в памяти защищённого архива НКМ-К;
- в данные, выгружаемые на внешние носители из памяти защищённого архива НКМ-К, автоматически включается дата, время, счетчик событий и квалифицированная электронная подпись.

5.3.4 Порядок выполнения ремонта тахографа путем замены НКМ-К

Ремонт тахографа путём замены НКМ-К должен производиться в случаях:

- выдачи тахографом диагностики об ошибках работы с НКМ-К;
- выдачи НКМ-К диагностики об ошибках в работе НКМ-К;
- компрометации ключевых документов НКМ-К;
- выработки НКМ-К установленного срока пользования.

При ремонте тахографа путём замены НКМ-К выполняются следующие операции:

- производится осмотр средств защиты тахографа (состояния кабелей, стыков подключения проводки, защитных пломб и клейм) и их состояние заносится в Акт выполненных работ в виде соответствующей записи: «средства защиты тахографа не нарушены» или «имеются следующие нарушения средств защиты тахографа»;
- при обнаружении нарушения средств защиты тахографа представитель мастерской должен:
    - сфотографировать имеющиеся нарушения, распечатать фотографии и приложить их к Акту выполненных работ;
    - сохранить цифровые фотографии для отчётности в архиве документов Мастерской;
    - уведомить владельца транспортного средства об обнаруженных нарушениях средств защиты тахографа;
    - если тахограф находится на гарантии – оформить Акт об отказе в гарантийном обслуживании на основании нарушения средств защиты тахографа;
- произвести демонтаж тахографа в соответствии с технической документацией поставщика тахографа;
- произвести вскрытие корпуса и замену НКМ-К;
- произвести операции установки, калибровки, активизации НКМ-К в установленном настоящими правилами порядке;

- осуществить уничтожение секретного ключа НКМ-К в мастерской с использованием сертифицированного оборудования в соответствии с технической документацией производителя НКМ-К.

6 Требования по обеспечению мер защиты

6.1 Требования к помещению

Оборудование помещений, предназначенных для хранения, встраивания и активизации НКМ-К должно исключать возможность бесконтрольного проникновения в эти помещения посторонних лиц и гарантировать сохранность находящихся в них носителей сведений, составляющих конфиденциальную информацию (средства криптографической защиты информации, ключевая информация).

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время, в них также могут устанавливаться кодовые и электронные замки и оборудоваться приспособления для опечатывания. Режимные помещения, в которых в нерабочее время хранятся носители сведений, составляющих конфиденциальную информацию, оснащаются охранной сигнализацией, связанной со службой охраны здания.

Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками. Для предотвращения просмотра извне окна оборудуются металлическими жалюзи.

Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает ответственное лицо. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящих требований.

Двери режимных помещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе ответственного лица.

Режимные помещения, в которых имеются технические средства, оборудуются в соответствии со специальными требованиями и рекомендациями по защите конфиденциальной информации, от утечки по техническим каналам (СТР-К).

Режимное помещение и размещаемое в нём оборудование (АРМы) должно быть аттестовано на соответствие требованиям по безопасности информации (т.е. иметь аттестаты соответствия).

Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

Режимные помещения, как правило, должны быть оснащены охранной и пожарной сигнализацией, связанной со службой охраны здания, а также системой видеонаблюдения.

Оборудование помещений средствами вентиляции и кондиционирования воздуха должно соответствовать санитарно-гигиеническими нормам СНиП, устанавливаемым законодательством Российской Федерации.

6.2 Требования к персоналу

К выполнению обязанностей встраивания и активизации НКМ-К допускаются лица, имеющие необходимый уровень квалификации для обеспечения защиты конфиденциальной информации с использованием НКМ-К.

При определении обязанностей должностных лиц необходимо учитывать, что безопасность хранения, обработки и передачи по каналам связи с использованием НКМ-К конфиденциальной информации обеспечивается:

- соблюдением персоналом режима конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых НКМ-К и ключевых документов к ним;
- точным выполнением требований к обеспечению безопасности конфиденциальной информации;
- надёжным хранением эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации;
- своевременным выявлением персоналом попыток посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых НКМ-К или ключевых документах к ним;
- немедленным принятием персоналом мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи НКМ-К, ключевых документов к ним, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

Объём и порядок ознакомления должностных лиц с конфиденциальной информацией определяется обладателем конфиденциальной информации.

Должен быть определён и утверждён список лиц, имеющих доступ к ключевой информации.

Обязанности между персоналом должны быть распределены с учётом персональной ответственности за сохранность НКМ-К, ключевой документации и конфиденциальных документов, а также за порученные участки работы.

6.3 Рекомендации по размещению оборудования (технических средств, АРМов) для обеспечения встраивания НКМ-К в

тахограф, активизации НКМ-К, технического обслуживания НКМ-К

При размещении технических средств, АРМов для обеспечения встраивания НКМ-К в тахограф, АРМов активизации тахографов с установленным НКМ-К, а также АРМов технического обслуживания НКМ-К должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, предназначенные для хранения, встраивания и активизации НКМ-К, а также по сохранению находящихся в этих помещениях конфиденциальных документов.

На АРМах, должно использоваться только лицензионное программное обеспечение (ПО) фирм-производителей.

Доступ персонала в режимные помещения должен быть регламентирован внутренним распорядком эксплуатирующей организации и должностными инструкциями.

Для исключения сбоев АРМов, вызванных отключением электропитания, необходимо обеспечить электропитание АРМов от источников бесперебойного питания достаточной мощности. Как минимум, мощности батарей источников бесперебойного питания должно хватать на время достаточное для корректного автоматического завершения работы АРМов.

На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утверждённые руководством организации, в которых предусматривается порядок вызова администрации, должностных лиц, вскрытие помещений, очередность и порядок эвакуации НКМ-2, конфиденциальных документов и дальнейшего их хранения.

6.4 Требования по защите от НСД при эксплуатации НКМ-К

6.4.1 Общие положения

Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах

функционирования, в том числе при проведении технического обслуживания тахографов в мастерской.

Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или администратором безопасности.

НКМ-К удовлетворяет «Требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классу КС3, «Требованиям к средствам электронной подписи» по уровню класса КС3.

Защита аппаратного и программного обеспечения АРМов от НСД при установке, активизации, техническом обслуживании НКМ-К является составной частью общей задачи обеспечения безопасности информации в системе тахографического контроля.

Наряду с применением технических средств защиты от НСД необходимо выполнение целого ряда мер, включающего в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установление соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

6.4.2 Организация работ по защите от НСД

Персонал, обеспечивающий встраивание НКМ-К в тахограф и активизацию НКМ-К, несет ответственность за соблюдение мер по защите от НСД. При обеспечении встраивания НКМ-К в тахограф, активизации тахографов с НКМ-К, в организации должен быть назначен администратор безопасности, на которого возлагаются задачи организации работ по использованию НКМ-К, выработки соответствующих инструкций для пользователей, а также контроль за соблюдением соответствующих требований.

Правом доступа к АРМам (по обеспечению встраивания НКМ-К в тахограф, активизации НКМ-К в тахографе, технического обслуживания

тахографа) должны обладать только определенные (выделенные для эксплуатации) лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя с документацией, обеспечивающей встраивание, активизацию и использование НКМ-К, а также с другими нормативными документами по обеспечению информационной безопасности.

При встраивании НКМ-К должны быть предусмотрены меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части тахографа (например, путём пломбирования тахографа).

При организации работ по защите информации от НСД необходимо учитывать следующие требования:

- необходимо разработать и применить политику назначения и смены паролей на АРМах;
- на АРМах, подключённых к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например, установка межсетевых экранов, организация VPN сетей и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации;
- организовать и использовать систему аудита, организовать регулярный анализ результатов аудита;
- организовать и использовать комплекс мероприятий антивирусной защиты