

**ПРОГРАММНО-АППАРАТНОЕ ШИФРОВАЛЬНОЕ  
(КРИПТОГРАФИЧЕСКОЕ) СРЕДСТВО  
БЛОК СКЗИ ТАХОГРАФА  
«Навигационно-криптографический модуль «НКМ-2.11 исполнение ИН»**

**Выписка из правил пользования**

1. Учёт и хранение НКМ 2.11 Исполнение ИН и криптографических ключей
2. Использование НКМ 2.11 Исполнение ИН
3. Требования по обеспечению мер защиты

# 1 Учёт и хранение НКМ и криптографических ключей

## 1.1 Учёт и хранение НКМ

### 1.1.1 Учёт и хранение НКМ при распространении

Организация поэкземплярного учёта НКМ возлагается на заказчика изделия.

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

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

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

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

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

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

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

### 1.1.2 Учёт и хранение НКМ при встраивании их в тахограф

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

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

2) Данные о заводских и регистрационных номерах НКМ и заводских номерах тахографов, в которые НКМ 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 в тахограф, должно обеспечивать:

- защиту от проникновения (усиленная дверь, решётки 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 производитель тахографа должен производить запись реквизитов покупателя (распространителя) тахографа в журнале поэкземплярного учёта НКМ.

### 1.1.3 Учёт НКМ при распространении и эксплуатации в составе тахографа

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

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

### 1.1.4 Учёт и хранение НКМ при техническом обслуживании тахографов

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

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

- защиту от проникновения (усиленная дверь, решётки 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 о заводском и регистрационном номерах НКМ, 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;
- об активизации тахографа и его заводской номер.

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

- сделать запись в журнале поэкземплярного учёта об установке НКМ с данным заводским и регистрационным номерами в тахограф, установленный 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, для установки его статуса в состояние «зabloкирован»;
- о заводском и регистрационном номерах НКМ, установленного взамен снятого, для установки его статуса в состояние «ТС активировано»;
- о заводском номере тахографа, в котором заменён НКМ.

## 1.2 Учёт и хранение криптографических ключей

### 1.2.1 Порядок учёта и хранения криптографических ключей НКМ

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

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

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

### 1.2.2 Порядок работы с ключами при техническом обслуживании и утилизации НКМ

1. При замене отработавшего срок эксплуатации НКМ уничтожение ключевой информации, содержащейся в НКМ осуществляется в автоматизированном режиме в соответствии с эксплуатационной документацией на НКМ. При этом сертификат открытого ключа НКМ сохраняется в составе НКМ для обеспечения проверки электронной подписи выгруженных данных из защищённого архива НКМ.

При выводе из эксплуатации НКМ до завершения его срока эксплуатации удаление ключевой информации должно осуществляться организацией, имеющей 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 с использованием сертифицированных ФСБ России средств. При этом сертификат открытого ключа НКМ должен быть сохранён в составе НКМ для обеспечения проверки электронной подписи выгруженных данных из защищённого архива НКМ.

Уничтожение ключевой информации НКМ 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», утверждённой приказом ФАПСИ от 13 июня 2001 г. № 152.

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

2. После уничтожения ключевой информации, НКМ с сохраненным сертификатом открытого ключа должен храниться у владельца транспортного средства. При этом срок хранения НКМ после его вывода из эксплуатации должен быть не менее года.

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

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

### 1.2.3 Порядок действий при компрометации ключевых документов

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

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

## 2 Использование НКМ

### 2.1 Порядок эксплуатации НКМ в составе тахографа

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

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

### 2.2 Порядок технического обслуживания НКМ

#### 2.2.1 Операции технического обслуживания НКМ

В ходе технического обслуживания НКМ могут выполняться следующие операции:

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

#### 2.2.2 Место проведения технологических операций и субъекты технического обслуживания

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

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

#### 2.3.3 Активизация и диагностика НКМ

При активизации НКМ должно обеспечиваться выполнение следующих требований:

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

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

- пользователь должен аутентифицироваться при помощи карты тахографа;

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

#### 2.3.4 Замена НКМ при обслуживании тахографа

Замена НКМ производится в случаях:

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

При замене НКМ 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;
- произвести операции установки, активизации НКМ в установленном настоящими правилами порядке;
- осуществить уничтожение ключевой информации НКМ в мастерской с использованием сертифицированного оборудования в соответствии с технической документацией производителя НКМ.

### 3. Требования по обеспечению мер защиты

#### 3.1 Требования к помещению

Оборудование помещений, предназначенных для хранения, встраивания и активизации НКМ 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 надёжное 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 решётками. 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 учёта 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 (АРМ) 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-гигиеническим нормам СНиП, устанавливаемым законодательством Российской Федерации.

#### 3.2 Требования к персоналу

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

При определении обязанностей должностных лиц необходимо учитывать, что безопасность хранения, обработки и передачи по каналам связи с использованием НКМ 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 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 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, 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, ключевой документации и конфиденциальных документов, а также за порученные участки работы.

### 3.3 Рекомендации по размещению оборудования (технических средств, АРМ) для обеспечения встраивания НКМ в тахограф, активизации НКМ, технического обслуживания НКМ

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

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

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, очерёдность и порядок эвакуации НКМ, конфиденциальных документов и дальнейшего их хранения.

## 3.4 Требования по защите от НСД при эксплуатации НКМ

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

Защита аппаратного и программного обеспечения АРМ от НСД при установке, активизации, техническом обслуживании НКМ 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.

### 3.4.2 Организация работ по защите от НСД

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

Правом доступа к АРМ (по обеспечению встраивания НКМ в тахограф, активизации НКМ 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, а также с другими нормативными документами по обеспечению информационной безопасности.

При встраивании НКМ 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 АРМ;

- на АРМ, 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.