**Ответы на вопросы из мастер-класса**

**С целью уточнения затронутых на мастер-классе вопросов, предлагаем актуальные ответы подготовленные экспертами проводившими вебинар.**

1. Вопрос: Тахограф с блоком НКМ это СКЗИ? Необходимо ли его учитывать? Как быть с разъяснением ФСБ России от 09.10.2013 №8/ЛЗ/2/2-2908?

Ответ: В разъяснении ЦЛСЗ ФСБ России от 09.10.2013г. №8/ЛЗ/2/2-2908 не упоминается о том, что ЦЛСЗ ФСБ России считает неактивированный блок НКМ не СКЗИ.

По мнению Центра лицензирования, условия использования неактивированного блока НКМ в тахографе выводят его из под действия Положения №313 О лицензировании… Но от этого неактивированный НКМ не перестает быть СКЗИ, со всеми вытекающими последствиями по необходимости его учета и контроля со стороны ФСБ России.

Дополнительно отмечаем, что согласно Приказу Минтранса №36 в состав бортового устройства тахографа включается блок СКЗИ с размещенной в нем, разработчиком блока, ключевой информацией. При этом блок СКЗИ еще не считается активизированным.

Так же, положения Приказа ФАПСИ №152 указывают на необходимость вести учет аппаратных средств, в которые установлены или к которым подключены СКЗИ, что ведет к необходимости учитывать и сами тахографы, в том числе и до их активации.

1. Вопрос: Необходимо ли вести учет тахографов без блока СКЗИ?

Ответ: Согласно Приказу ФАПСИ №152, учету подлежат устройства, в которых размещены или к которым подключены СКЗИ. Прямых указаний на необходимость учитывать устройство (тахограф) до размещения в нем блока СКЗИ отсутствуют. Но учитывая, что в тахографе однозначно в дальнейшем будет использоваться блок СКЗИ и карта водителя с персональными данными, следует вести учет такого тахографа (без блока СКЗИ). Необходимость учета продиктована, в том числе:

* приказом ФСБ от 10 июля 2014 года №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
* «Методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденными руководством 8 Центра ФСБ России (№149/7/2/6-432 от 31.03.2015);

Учет таких тахографов (без блока СКЗИ) необходим с целью исключения внесения несанкционированных изменений в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности представляющие среду функционирования СКЗИ (далее - СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

Учет СФ является составной частью общей задачи обеспечения безопасности информации в системе, в состав которой входит СКЗИ.

Опираясь на вышеизложенное, считаем целесообразным ставить на учет оборудование, к которому предполагается дальнейшее подключение СКЗИ и функциональное применение которого без СКЗИ не осуществляется.

1. Вопрос: Как организовывать доставку тахографа от места активации до места установки?

Ответ: Доставка должна быть осуществлена ответственным сотрудником мастерской. После установки тахографа и его активизации, ответственный представитель собственника автотранспортного средства расписывается в сопроводительном документе о получении тахографа. Реквизиты сопроводительного документа заносятся в журналы учета.

1. Вопрос: Если приехала организация на активацию с уже установленным тахографом, как мы ставим на приход не наш тахограф? У нас своих тахографов нет. Что мы должны учитывать? Мы только активируем тахограф.

Ответ: СКЗИ является в том числе и ключевая информация, заносимая в блок НКМ тахографа. Факт её формирования и внесения в блок НКМ тахографа и регистрируется в соответствующем журнале учета СКЗИ, в котором указываются и учетные данные самого тахографа.

1. Вопрос: Каков порядок учета СКЗИ в журналах, лицевых счетах пользователей?

Ответ: Инструкция по порядку учета СКЗИ (тахографов, карт тахографов) и рекомендации размещены на сайте <http://naviport.info/>

1. Вопрос: Как сотрудники ФСБ России при проведении проверок относятся к ведению учета в электронном виде?

Ответ: Ведение журналов учета в электронном виде нормативной документацией не запрещено. Но в настоящее время, при проведении проверок, сотрудники ФСБ России ожидают увидеть в мастерской журналы в бумажном виде.

 Рассмотрите вариант автоматизации учета СКЗИ и ведение электронных журналов учета и лицевых счетов с периодическим выводом их на печать и подшивкой. В регистрах журналов при этом проставляются реквизиты документов приема и передачи тахографов.

 Согласно нашему опыту ведения автоматизированного учета СКЗИ, включая контроль ресурсов аттестованной автоматизированной системы и порядка обработки персональных данных, внесение данных по полученным, установленным и активизированным тахографам и выданным картам тахографа в единую электронную базу данных позволяет не только автоматизировать ведение журналов учета и лицевых счетов, но и вести и контролировать историю договорных отношений с клиентами с отражением различных технических деталей. При накоплении значительных объемов данных, электронная база данных позволяет комфортно вести оперативный учет деятельности.

1. Вопрос: Является ли активация СКЗИ тахографов собственных автомобилей лицензируемой деятельностью?

Ответ: Согласно Постановлению №313 О лицензировании…, только обслуживание СКЗИ для собственных нужд не лицензируется. Для осуществления активации СКЗИ тахографов лицензия нужна.

1. Вопрос: Если в мастерской уволился штатный специалист по информационной безопасности или принимается новый надо ли сообщать об этом в ФСБ России?

Ответ: Нормативные требования ФСБ России, обязывающие лицензиатов ФСБ России, в том числе мастерские тахографического контроля, это делать, отсутствуют.

1. Вопрос: Если специалисты ИБ с необходимым стажем уволены мастерской, но остались двое других действующих сотрудников, прошедших переподготовку по ИБ, но не имеющих необходимого стажа 3 года. Чем это грозит при проверке?

Ответ: В рамках осуществления деятельности по п.п.12, 20 Постановления №313 О лицензировании… это будет считаться грубым нарушением. По п. 21 Постановления, мастерская соответствует лицензионным требованиям. Грубое нарушение наказывается штрафом до 40000,00 руб. Дополнительно, мастерской будет предписано в 30-ти дневный срок устранить несоответствие.

 Из практики можно отметить, что наличие сотрудников с необходимым образованием, но без стажа, покажет проверяющим желание мастерской не игнорировать лицензионные требования, что может снизить сумму штрафа, но не отменить его.

 Рассмотрите возможность устроить в штат специалистов ИБ с необходимым стажем по совместительству.

1. Вопрос: Как происходит аннулирование лицензии (по желанию мастерской), будет ли проводиться проверка в этом случае?

Ответ: Аннулирование лицензии осуществляется по заявлению (форма заявления указана в указанном ниже Регламенте) с приложением лицензии. Порядок указан в Административном регламенте Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности, утвержденном Приказом Федеральной службы безопасности Российской Федерации от 30 августа 2012 г. N 440 г. Москва. Проверка при аннулировании лицензии данным Регламентом не предусмотрена.

1. Вопрос: Какой штат специалистов ИБ должен быть при работе с картами тахографов, при обработке персональных данных?

Ответ: Согласно Постановлению №313 О лицензировании…, при работе с картами тахографов в штате должно быть не менее двух специалистов ИБ. К стажу требования не предъявляются.

Проверяющие со стороны Роскомнадзора дополнительно могут указать на необходимость наличия хотя-бы одного сотрудника в организации отвечающего за безопасную обработку персональных данных, прошедшего соответствующее обучение.

Проверяющие со стороны ФСБ России дополнительно могут потребовать наличия протоколов проверки знаний сотрудников мастерской, допущенных к работе со СКЗИ правилам работы с ними. Это предусмотрено Приказом ФАПСИ №152.

1. Вопрос: Должен ли водитель писать дополнительное согласие на обработку персональных данных или достаточно того, что в заявлении на выдачу карты?

Ответ: Дополнительное согласие от водителя брать не нужно. В заявлении на выдачу карты предусмотрите все возможные варианты обработки персональных данных.

 С основами защищенной обработки персональных данных можно ознакомиться в соответствующем разделе на сайте <http://naviport.info/>

1. Вопрос: При изменении программной или аппаратной конфигурации автоматизированного рабочего места (ПО/СКЗИ/СЗИ от НСД и пр.), в том числе изменение тех. паспорта рабочего места, необходимо ли проводить переаттестацию автоматизированной системы?

Ответ: Согласно нормативным требованиям, переаттестация необходима при изменении условий эксплуатации, состава программно-аппаратных ресурсов, могущих повлиять на безопасность. Порядок действий в этом случае предусматривает направление запроса в организацию проводившую аттестацию. В случае возможности, эта организация может согласовать внесение изменений в аттестованную систему без проведения переаттестации. Изменения в тех. паспорт автоматизированной системы мастерская может внести самостоятельно.

1. Вопрос: Нужно ли ежегодно производить контроль рабочего места специализированной организацией?

Ответ: Аттестация автоматизированного рабочего места по требованиям безопасности конфиденциальной информации проводится не реже одного раза в три года, или при изменении условий эксплуатации, состава программно-аппаратных ресурсов, могущих повлиять на безопасность. Ежегодно необходимо проводить текущий контроль защищенности. Это можно делать самостоятельно.

Аттестацию должен проводить лицензиат ФСТЭК России с правом проводить соответствующие работы. При этом, не обязательно чтобы это был аккредитованный орган по аттестации, который в т.ч. имеет право проводить аттестацию объектов, обрабатывающих гос. тайну.

Оценка эффективности мер по защите персональных данных, в случае их обработки, так же проводится не реже одного раза в три года. Периодический контроль защищенности в этом случае так же проводится с периодичностью не реже одного раза в год.

1. Вопрос: Какие программные или аппаратные средства защиты информации, средства криптографической защиты информации могут быть в мастерской?

Ответ: В мастерской могут быть следующие средства защиты: сертифицированный антивирус, электронная подпись, средства от несанкционированного доступа, такие как SecretNet, Dallas Lock, АМДЗ «Аккорд» и другие. Кроме того, Мастерская использует СКЗИ «Карта тахографа «Диамант» (Сертификат ФСБ России СФ/124-2820 действителен до 30.03.2018) и СКЗИ для организации защищенного канала передачи данных (USB-устройство С-Терра «Пост») (Сертификат ФСБ России [Сертификат ФСБ России № СФ/124-2516 (КС2)](http://www.s-terra.ru/upload/medialibrary/bdd/fsb_124-2516_gate-st-kc2.jpg) действителен до 01.12.2017)

1. Вопрос: Согласно каким статьям КоАП, какая предусмотрена административная ответственность за нарушения?

**Статья 13.6.** Использование средств связи или несертифицированных средств кодирования (шифрования), не прошедших процедуру подтверждения их соответствия установленным требованиям

1. Использование в сетях связи несертифицированных средств связи или несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети "Интернет", если законодательством предусмотрена их обязательная сертификация, - влечет наложение административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей с конфискацией несертифицированных средств связи либо без таковой; на должностных лиц - от пятнадцати тысяч до тридцати тысяч рублей с конфискацией несертифицированных средств связи либо без таковой; на юридических лиц - от шестидесяти тысяч до трехсот тысяч рублей с конфискацией несертифицированных средств связи либо без таковой.

2. Использование в сетях связи средств связи без декларации о соответствии, если законодательством не предусмотрена их обязательная сертификация, - влечет наложение административного штрафа на должностных лиц в размере от пятнадцати тысяч до тридцати тысяч рублей с конфискацией незадекларированных средств связи либо без таковой; на юридических лиц - от шестидесяти тысяч до ста пятидесяти тысяч рублей с конфискацией незадекларированных средств связи либо без таковой.

**Статья 13.12.** Нарушение правил защиты информации

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от одной тысячи до одной тысячи пятисот рублей; на должностных лиц - от одной тысячи пятисот до двух тысяч пятисот рублей; на юридических лиц - от пятнадцати тысяч до двадцати тысяч рублей.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до двух тысяч пятисот рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от двух тысяч пятисот до трех тысяч рублей; на юридических лиц - от двадцати тысяч до двадцати пяти тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой.

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от двух тысяч до трех тысяч рублей; на юридических лиц - от двадцати тысяч до двадцати пяти тысяч рублей.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от трех тысяч до четырех тысяч рублей; на юридических лиц - от двадцати тысяч до тридцати тысяч рублей с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

5. Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), - влечет наложение административного штрафа на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от двух тысяч до трех тысяч рублей или административное приостановление деятельности на срок до девяноста суток; на должностных лиц - от двух тысяч до трех тысяч рублей; на юридических лиц - от двадцати тысяч до двадцати пяти тысяч рублей или административное приостановление деятельности на срок до девяноста суток.

6. Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных [частями 1](#Par4333), [2](#Par4336) и [5](#Par4345) настоящей статьи, - влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц - от одной тысячи до двух тысяч рублей; на юридических лиц - от десяти тысяч до пятнадцати тысяч рублей.

7. Нарушение требований о защите информации, составляющей государственную тайну, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных [частями 3](#Par4339) и [4](#Par4342) настоящей статьи, если такие действия (бездействие) не содержат уголовно наказуемого деяния, - влечет наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц - от трех тысяч до четырех тысяч рублей; на юридических лиц - от пятнадцати тысяч до двадцати тысяч рублей.

Примечание. Понятие грубого нарушения устанавливается Правительством Российской Федерации в отношении конкретного лицензируемого вида деятельности.

**Статья 13.13.** Незаконная деятельность в области защиты информации

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; на должностных лиц - от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц - от десяти тысяч до двадцати тысяч рублей с конфискацией средств защиты информации или без таковой.

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии - влечет наложение административного штрафа на должностных лиц в размере от четырех тысяч до пяти тысяч рублей; на юридических лиц - от тридцати тысяч до сорока тысяч рублей с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

**Статья 14.1.** Осуществление предпринимательской деятельности без государственной регистрации или без специального разрешения (лицензии)

1. Осуществление предпринимательской деятельности без государственной регистрации в качестве индивидуального предпринимателя или без государственной регистрации в качестве юридического лица - влечет наложение административного штрафа в размере от пятисот до двух тысяч рублей.

2. Осуществление предпринимательской деятельности без специального разрешения (лицензии), если такое разрешение (такая лицензия) обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от двух тысяч до двух тысяч пятисот рублей с конфискацией изготовленной продукции, орудий производства и сырья или без таковой; на должностных лиц - от четырех тысяч до пяти тысяч рублей с конфискацией изготовленной продукции, орудий производства и сырья или без таковой; на юридических лиц - от сорока тысяч до пятидесяти тысяч рублей с конфискацией изготовленной продукции, орудий производства и сырья или без таковой.

3. Осуществление предпринимательской деятельности с нарушением требований и условий, предусмотренных специальным разрешением (лицензией), - влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи пятисот до двух тысяч рублей; на должностных лиц - от трех тысяч до четырех тысяч рублей; на юридических лиц - от тридцати тысяч до сорока тысяч рублей.

4. Осуществление предпринимательской деятельности с грубым нарушением требований и условий, предусмотренных специальным разрешением (лицензией), - влечет наложение административного штрафа на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от четырех тысяч до восьми тысяч рублей или административное приостановление деятельности на срок до девяноста суток; на должностных лиц - от пяти тысяч до десяти тысяч рублей; на юридических лиц - от ста тысяч до двухсот тысяч рублей или административное приостановление деятельности на срок до девяноста суток.

Примечания:

1. Понятие грубого нарушения устанавливается Правительством Российской Федерации в отношении конкретного лицензируемого вида деятельности.

2. Лицо освобождается от административной ответственности при выявлении факта совершения им действий (бездействия), содержащих признаки состава административного правонарушения, предусмотренного настоящей статьей или [статьями 15.1](#Par5583), [15.3](#Par5595) - [15.6](#Par5628), [15.11](#Par5681), [15.25](#Par5975) настоящего Кодекса, при условии, если это лицо является декларантом или лицом, информация о котором содержится в специальной декларации, поданной в соответствии с Федеральным законом "О добровольном декларировании физическими лицами активов и счетов (вкладов) в банках и о внесении изменений в отдельные законодательные акты Российской Федерации", и если такие действия (бездействие) связаны с приобретением (формированием источников приобретения), использованием либо распоряжением имуществом и (или) контролируемыми иностранными компаниями и (или) с совершением валютных операций и (или) зачислением денежных средств на счета (вклады), информация о которых содержится в специальной декларации.

(примечания введены Федеральным законом от 08.06.2015 N 140-ФЗ)

1. Вопрос: Где размещается план проверок ФСБ России?

Ответ: Ссылка на размещение плана проверок в сети интернет:

http://www.fsb.ru/fsb/science/single.htm%21id%3D10437686%40fsbResearchart.html

1. Вопрос: Где размещается план проверок Роскомнадзора?

Ответ: Ссылка на размещение плана проверок в сети интернет:

<https://rkn.gov.ru/plan-and-reports/>

1. Вопрос: Как правильно провести аттестацию АРМ на соответствие ИБ, какие документы подготовить по данному вопросу, так чтобы они устроили проверяющего ФСБ России?

Ответ: Как было указано выше, аттестацию должен проводить лицензиат ФСТЭК России с правом проводить соответствующие работы. При этом, не обязательно чтобы это был аккредитованный орган по аттестации, который в т.ч. имеет право проводить аттестацию объектов, обрабатывающих гос. тайну.

 Как правило, организации проводящие работы по аттестации осуществляют предварительную подготовку автоматизированной системы (АС) к аттестации, включающую в себя разработку следующего минимального комплекта документов:

 - Приказы по организации об утверждении системы допусков к ресурсам АС;

 - Инструкции администратору ИБ и пользователям в части регламентирования порядка защищенной обработки информации;

 - Приказ об определении контролируемой зоны;

 - Акты установки средств защиты информации;

- Акт классификации АС;

 - Матрица доступа к ресурсам АС;

 - Технический паспорт АС.

На этапе проведения аттестационных испытаний готовятся:

 - Программа и методики аттестационных испытаний;

 - Протоколы аттестационных испытаний;

 - Заключение по итогам аттестационных испытаний.

При наличии оснований, по итогам аттестационных испытаний оформляется аттестат соответствия АС требованиям по защите информации.