Порядок

организации и проведения работ

по обеспечению безопасности персональных данных

при их обработке в информационных системах персональных данных в организациях, осуществляющих деятельность по установке, поверке, техническому обслуживанию и ремонту тахографов, а также в пунктах выдачи карт водителя

1. ОБЩИЕ ПОЛОЖЕНИЯ
	1. Назначение Порядка

Настоящий Порядок (далее – Порядок) описывает организацию и проведение работ по защите информации, содержащей персональные данные (ПДн), на объектах информатизации в организациях, осуществляющих деятельность по установке, поверке, техническому обслуживанию и ремонту тахографов, а также в пунктах выдачи карт водителя (далее - Мастерская) как в период их создания, так и в процессе повседневной эксплуатации.

* 1. Технологическая карта организации работ
		1. Определить какие ПДн обрабатываются в Мастерской (п.п.2.1.1 Порядка);
		2. Определить в каких целях ведется обработка ПДн в Мастерской (п.п.2.1.2 Порядка);
		3. Определить в течение какого срока будет вестись обработка ПДн, включая их хранение (п.п.2.1.3 Порядка);
		4. Определить уровни защищенности ПДн;
		5. Определить ответственных лиц за обеспечение безопасности ПДн (п.п.2.1.4 Порядка);
		6. Определить круг лиц, допущенных к обработке ПДн (п.п.2.1.5 Порядка);
		7. Обеспечить контролируемый доступ в помещения, где обрабатываются ПДн (п.п.2.1.6 Порядка);
		8. Провести обучение сотрудников правилам обработки ПДн (п.п.2.1.7 Порядка);
		9. Установить персональную ответственность за нарушение правил обработки ПДн (п.п.2.1.8 Порядка);
		10. Обеспечить учёт применяемых средств защиты ПДн (п.п.2.1.9 Порядка);
		11. Обеспечить учёт носителей ПДн (п.п.2.1.10 Порядка);
		12. Разработать комплект организационно-распорядительных документов по обеспечению безопасности ПДн (п.п.2.1.11 Порядка);
		13. Разработать комплект технических документов по защите ПДн, установить и сконфигурировать необходимые средства защиты информации (п.п.2.1.12, п.2.2 Порядка);
		14. Провести Оценку эффективности принимаемых мер по обеспечению безопасности ПДн (п.п.2.2.2. Порядка);
		15. Подать Уведомление об обработке ПДн в Уполномоченный орган (п.п.2.1.13 Порядка);
		16. Обеспечить текущий контроль безопасности обрабатываемых ПДн (п.2.3 Порядка).
1. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАсНОСТИ персональных данных ПРИ ИХ ОБРАБОТКЕ В ИСПДН
	1. Организационные мероприятия

Статья 18.1 Федерального закона «О персональных данных» требует от операторов ПДн иметь локальные акты и политику, регламентирующую обработку и защиту ПДн в информационных системах персональных данных (ИСПДн). **Точного перечня необходимых документов не предполагается** и жестких требований о количестве подлежащих разработке локальных актов оператора действующим законодательством не установлено.

Организационные мероприятия по защите ПДн включают в себя:

* + 1. Определение перечня ПДн, обрабатываемых в ИСПДн.

Устанавливается наличие и состав ПДн, которые обрабатываются в Мастерской.

* + 1. Определение цели обработки ПДн.

Определяются цели обработки ПДн: трудовые отношения с работниками; оказание услуг в области тахографического контроля и т.д.

* + 1. Определение сроков обработки и хранения ПДн.

Хранение персональных данных должно осуществляться не дольше, чем этого требуют цели их обработки, по достижении которых ПДн подлежат уничтожению.

По результатам анализа информации, обрабатываемой в Мастерской, и реализации мероприятий, указанных в п.п. 2.1.1-2.1.3, определяется уровень защищенности ПДн при их обработке в ИСПДн в соответствии с постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

* + 1. Определение ответственных за обеспечение безопасности ПДн.

Ответственный за обеспечение безопасности ПДн и администратор безопасности ПДн определяются приказом руководителя Мастерской.

Ответственный за обеспечение безопасности ПДн разрабатывает и осуществляет мероприятия (организовывает и контролирует осуществление мероприятий) по обеспечению безопасности ПДн при их обработке в ИСПДн.

Задачи, функции, обязанности, права и ответственность администратора безопасности ПДн определяются Инструкцией администратору безопасности ПДн.

* + 1. Определение круга лиц, допущенных к обработке ПДн.

Руководителями структурных подразделений составляется список (перечень) сотрудников, доступ которых к обрабатываемым в ИСПДн персональным данным необходим для выполнения служебных (трудовых) обязанностей. Перечень лиц, допущенных к обработке ПДн, утверждается руководителем Мастерской.

К обработке ПДн допускаются сотрудники Мастерской, подготовленные к работе с информацией, требующей защиты (пользователи ИСПДн).

Ответственным за обеспечение безопасности ПДн разрабатывается разрешительная система доступа данных пользователей к информационным ресурсам ИСПДн.

Права доступа администратору безопасности ПДн и пользователям ИСПДн оформляются в виде матрицы доступа к защищаемым информационным ресурсам.

* + 1. Организация доступа в помещения, где осуществляется обработка ПДн.

Необходимо исключить возможность несанкционированного доступа и пребывания в помещениях, где обрабатываются ПДн, а также к техническим средствам обработки ПДн, хищения и нарушения работоспособности технических средств обработки ПДн, хищения носителей информации.

Порядок охраны помещений ИСПДн, доступа в эти помещения определяется соответствующей Инструкцией о порядке допуска в помещения ИСПДн.

* + 1. Обучение сотрудников.

Не реже одного раза в год необходимо проводить обучение пользователей ИСПДн правилам обработки ПДн в соответствии с действующим законодательством, а также правилам работы со средствами защиты информации, применяемыми в ИСПДн, в соответствии с документацией (инструкции, руководства и т.п.), прилагаемой к таким средствам защиты информации.

Обучение может проводиться в форме совещаний, обучающих занятий, семинаров, инструктажей, методической помощи и практических занятий на месте. Обучение может проводиться в ходе периодических (плановых) и внеплановых проверок состояния обеспечения безопасности ИСПДн на местах.

Первичные инструктажи проводятся с пользователями ИСПДн при поступлении на работу сотрудника в структурное подразделение Мастерской, в котором происходит обработка персональных данных в ИСПДн.

Ответственным за организацию обучения и оказание методической помощи пользователям ИСПДн в Мастерской является ответственный за обеспечение безопасности ПДн.

Для проведения обучающих мероприятий могут привлекаться администратор безопасности ПДн, а также специалисты организаций, оказывающих услуги в области защиты информации.

Обучение по отдельным направлениям обеспечения защиты ПДн, как в организационной, так и технической частях, может проводиться образовательными организациями в форме повышения осведомленности, повышения квалификации и т.п. с выдачей подтверждающих документов установленного образца.

К работе в ИСПДн допускаются только сотрудники, прошедшие первичный инструктаж обеспечения безопасности ПДн в ИСПДн и показавшие твёрдые теоретические знания и практические навыки.

В целях изучения практических вопросов обеспечения безопасности в реально действующих информационных системах и ознакомления с новыми решениями в области информационной безопасности ответственный за обеспечение безопасности ПДн, администратор безопасности ПДн и другие специалисты, обеспечивающие безопасность персональных данных, должны периодически проходить курсы повышения квалификации (переподготовки) в области информационной безопасности.

Кроме того, данные сотрудники должны самостоятельно изучать необходимые для работы документы, а также современные средства защиты информации.

Мероприятия по обучению сотрудников Мастерских по вопросам защиты информации, в т.ч. ПДн могут осуществляться в электронной форме с использованием технологий удаленного доступа при использовании специализированного программного обеспечения (например, А(И)С©, см. п.п.2.5 Порядка).

* + 1. Установление персональной ответственности за нарушения правил обработки ПДн.

В должностные инструкции пользователям ИСПДн должны быть внесены дополнения в части персональной ответственности за нарушение правил обработки ПДн.

* + 1. Учёт применяемых технических средств защиты ПДн.

При выборе технических (аппаратных, программных и программно-аппаратных) средств защиты предпочтительнее использовать сертифицированные средства защиты информации. Перечень используемых средств защиты с указанием их заводского номера, сведений о сертификате соответствия, месте и дате установки приводится в Техническом паспорте на ИСПДн.

Учёт применяемых технических средств защиты ПДн может быть организован при использовании специализированного программного обеспечения.

* + 1. Учёт носителей ПДн.

В обязательном порядке должен быть организован учёт всех защищаемых носителей ПДн с помощью их маркировки и с занесением учётных данных в Журнал регистрации, учёта и выдачи носителей информации.

Запрещается несанкционированное использование съёмных носителей информации, содержащей ПДн, и использование незарегистрированных носителей информации, содержащей ПДн.

Учёт носителей ПДн может быть организован при использовании специализированного программного обеспечения.

* + 1. Разработка организационно-распорядительных документов по обеспечению безопасности ПДн.

В рамках реализации мер по обеспечению безопасности ПДн должны быть разработаны и приняты организационные документы. Шаблоны таких документов представлены на сайте <http://naviport.info>.

Ответственность за организацию разработки организационно-распорядительных документов возлагается на ответственного за обеспечение безопасности ПДн.

* + 1. Разработка технических документов по обеспечению безопасности ПДн.

В рамках реализации мер по обеспечению безопасности ПДн должны быть разработаны и приняты следующие технические документы:

* модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных по методике ФСТЭК России и ФСБ России;
* технический паспорт на ИСПДн.

К разработке частной модели угроз рекомендуем привлечь организации, обладающие соответствующими лицензиями ФСТЭК России и ФСБ России.

Разработка и ведение технического паспорта на ИСПДн, а так же, подготовка модели угроз могут быть организованы при использовании специализированного программного обеспечения.

* + 1. Подача Уведомления об обработке ПДн в Уполномоченный орган по защите прав субъектов ПДн.

Ответственность за своевременную подачу Уведомления об обработке ПДн в Уполномоченный орган по защите прав субъекта ПДн возлагается на ответственного за обеспечение безопасности ПДн.

Подготовка Уведомления может быть организована при использовании специализированного программного обеспечения.

* 1. Технические мероприятия

Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации (СЗИ). При обработке ПДн с использованием средств автоматизации применение СЗИ является обязательным условием, а их количество и степень защиты определяется на основании Акта определения уровня защищенности ПДн в ИСПДн и частной модели угроз безопасности ПДн при их обработке в ИСПДн по методике ФСТЭК России и ФСБ России.

* + 1. Требования к техническим и программным средствам.

Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в ИСПДн, могут проходить в установленном порядке процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

* + 1. Необходимость создания системы защиты ПДн.

Создание системы защиты ПДн (СЗПДн) является необходимым условием обеспечения безопасности ПДн, в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиями к обеспечению безопасности ПДн для ИСПДн соответствующего класса и/или не покрывают всех угроз безопасности ПДн для данной ИСПДн.

Целью создания СЗПДн является: обеспечение защиты информации, содержащей ПДн, от утечки по техническим каналам и от несанкционированного доступа. Защита осуществляется путём выполнения комплекса организационных и технических мероприятий, в соответствии с требованиями государственных стандартов, руководящих и нормативно-методических документов ФСТЭК России, реализуемых в рамках создаваемой СЗПДн.

СЗПДн должна включать:

* организационные меры и технические средства защиты информации;
* средства предотвращения:
	+ несанкционированного доступа к информации;
	+ утечки информации по техническим каналам;
	+ программно-технических воздействий на технические средства обработки персональных данных;
* меры по криптографической защите информации;
* используемые в ИСПДн информационные технологии.

Результатом создания СЗПДн является подтверждение соответствия ИСПДн требованиям безопасности персональных данных путем **Оценки эффективности** принимаемых мер по обеспечению безопасности персональных данных которая может проводиться в формах добровольной **Аттестации** по требованиям безопасности информации в системе сертификации ФСТЭК России, а также в других формах, выбираемых самой Мастерской, в виде самооценки (например, формах приемо-сдаточных испытаний СЗПДн, совместной оценки комиссией, состоящей из представителей Разработчика и Заказчика СЗПДн, и т. д.).

Процедура проведения самооценки может быть автоматизирована при использовании специализированного программного обеспечения.

При проведении Мастерской самооценки принимаемых мер, рекомендуется привлекать к работе в комиссии, в качестве экспертов, специалистов по защите информации, в т.ч. лицензиатов ФСТЭК России.

Одной из форм подтверждения соответствия проводимой самооценки нормативным требованиям может быть заключение лицензиата ФСТЭК России по результатам проведенной самооценки Мастерской.

Аттестация объекта информатизации по требованиям безопасности информации представляет собой комплекс организационно-технических мероприятий, в результате которых подтверждается, что на аттестационном объекте выполнены требования по безопасности информации, заданные в нормативно-технической документации, утверждённые государственными органами обеспечения безопасности информации и контролируемые при аттестации.

В настоящее время, процедура Аттестации проводится в обязательном порядке для государственных и муниципальных учреждений.

Аттестация проводится лицензиатом ФСТЭК России, имеющем разрешение на этот вид деятельности, в установленном законодательством порядке.

Результатом Аттестации объекта информатизации (ИСПДн) является получение «Аттестата соответствия требованиям по безопасности информации персональных данных при их обработке в информационной системе персональных данных <наименование ИСПДн>» (далее – Аттестат соответствия).

Владелец аттестованного объекта информатизации несёт ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

* 1. Контроль обеспечения безопасности (защиты) ПДн при создании СЗПДн

Задачами контроля обеспечения безопасности (защиты) ПДн являются:

* контроль выполнения требований безопасности ПДн в ИСПДн,
* координация действия подразделений Мастерской по организации и обеспечению безопасности ПДн;
* предупреждение, выявление и пресечение выявленных нарушений.

Общее руководство работами по обеспечению безопасности ПДн осуществляет руководитель Мастерской.

Ответственный за обеспечение безопасности ПДн (администратор безопасности ПДн) выполняет:

* анализ состояния и определение требований к защищённости различных ИСПДн;
* выбор методов и средств обеспечения защиты ПДн;
* разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам обеспечения безопасности ПДн;
* администрирование и контроль применения средств защиты информации, а также поддержку функционирования средств, технологий и процессов при обработке ПДн;
* разработку требований по обеспечению безопасности ПДн (создание/модернизацию СЗПДн);
* организацию проведения работ по защите ПДн;
* контроль выполнения требований по обеспечению безопасности ПДн и эффективности предусмотренных мер защиты.

Обязанности пользователей ИСПДн определяются их должностными инструкциями, Инструкцией администратору безопасности ПДн, Инструкцией по работе пользователям ИСПДн и другими организационно-распорядительными документами, разрабатываемыми в соответствии с настоящим Порядком.

Пользователи ИСПДн не имеют права использовать в неслужебных целях информационные ресурсы ИСПДн, обязаны соблюдать конфиденциальность (не разглашать, не допускать распространения) ставшей им известной в связи с исполнением должностных обязанностей информации ограниченного доступа (персональных данных).

Обеспечение текущего контроля состояния системы защиты ПДн может быть осуществлено с использованием специализированного программного обеспечения (например, А(И)С©, см. п.п.2.5 Порядка);

* 1. Привлечение сторонних организаций

Разработка и осуществление мероприятий СЗПДн может осуществляться как специалистами по защите информации Мастерской, так и специализированными организациями, имеющими лицензии ФСТЭК России, ФСБ России на соответствующий вид деятельности.

* 1. Использование сервисов информационной системы А(И)С©

Организация и проведение работ по защите ПДн может осуществляться Мастерской самостоятельно, с использованием сервисов информационной системы А(И)С© и с привлечением технических специалистов сопровождающих эту систему.

Сервисы информационной системы А(И)С© функционируют в рамках деятельности Органа криптографической защиты информации и используются в том числе для обеспечения безопасности ПДн.

Основные направления задач, решаемых с помощью информационной системы А(И)С©:

* разработка и ведение организационно-распорядительной и эксплуатационно-технической документации по объекту информатизации;
* обеспечение комфортного ведения учета производственной деятельности Мастерской при накоплении значительных объемов данных, с возможностью ведения истории в различных разрезах учета, в т.ч. по заказчикам, по объектам учета и т.п.
* обеспечение готовности и самооценка эффективности принимаемых мер по обеспечению безопасности ПДн в информационной системе;
* организация обучения и повышения осведомленности персонала по вопросам информационной безопасности;
* систематизация и учет программно-аппаратных, информационных ресурсов, средств криптографической защиты информации;
* обеспечение выполнения требований ФСБ России к обороту и эксплуатации СКЗИ;
* тестирование систем информационной безопасности сетевой инфраструктуры организации;
* администрирование систем информационной безопасности сетевой инфраструктуры организации.

А(И)С© доступна для ознакомления по адресу в сети Интернет: <https://www.zs-info.ru/> в разделе защита персональных данных.