ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

В МАСТЕРСКИХ, ОСУЩЕСТВЛЯЮЩИХ ДЕЯТЕЛЬНОСТЬ ПО УСТАНОВКЕ, ПРОВЕРКЕ, ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ И РЕМОНТУ ТАХОГРАФОВ, А ТАКЖЕ В ПУНКТАХ ВЫДАЧИ КАРТ ВОДИТЕЛЯ

ВВОДНАЯ ЧАСТЬ

Подготовил: Андрей Богданов, эксперт по защите информации, руководитель Краснодарского отделения Экспертно-образовательного частного учреждения «Южная техническая комиссия»

Защита персональных данных в мировой практике

Роскомнадзор
#пд

Ок, не знаете. Рассказываем.

В 1948 г. ООН приняла Всеобщую декларацию прав человека, в которой указано, что «никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь произвольным посягательством на его честь и репутацию».

Статья Декларации получила развитие в Конвенции «О защите физических лиц при автоматизированной обработке персональных данных» (1981 г.). Все страны, ратифицировавшие ее, обязаны предусмотреть один или более наблюдательный орган, который несет ответственность за осуществление принципов Конвенции.

В связи с этим Федеральным законом № 152-ФЗ «О персональных данных» был введен Уполномоченный орган по защите прав субъектов персональных данных в РФ, который обеспечивает контроль и надзор за соответствием обработки персональных данных.

В настоящий момент этим органом является Роскомнадзор.

Законодательство о персональных данных в Российской Федерации

В Российской Федерации с 1 июля 2011 года вступил в силу закон №152-ФЗ от 27 июля 2006 года «О персональных данных». В сферу действия данного закона попадают все юридические и физические лица, которые обрабатывают персональные физических лиц. Закон требует, в частности, чтобы каждая организация, владеющая персональными данными, обеспечила их конфиденциальность. В случае нарушения положений закона компания может лишиться лицензии, аккредитаций и подвергнуться судебному преследованию со стороны граждан, чьи приватные записи были скомпрометированы. За неисполнение закона предусмотрена гражданская, уголовная, административная, дисциплинарная и иная предусмотренная законодательством РФ ответственность.

Что такое персональные данные?
любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу

Относятся ли к персональным данным в частности следующие документы для получения карты водителя:

* Копия ИНН (идентификационный номер налогоплательщика).
* Фотография 3.5 Х 4.5
* Копии паспорта (основная страница и прописка) водителя.
* Копия водительского удостоверения, с двух сторон.
* Копия СНИЛС (страховой номер индивидуального лицевого счета)
* Заявление на получение карты водителя.
* Сама карта водителя

Да, относятся,
но остаются проблемы:

- что точно необходимо относить к персональным данным
- относить ли фотографию к биометрическим персональным данным
- как обращаться с картами водителя, на которых осуществлена запись биометрических персональных данных водителя, а также как их хранить вне информационных систем персональных данных
- высокая вероятность быть привлеченным к ответственности за невыполнение требований по организации обработки персональных данных, защите информации

Опираясь на имеющуюся судебную практику, давайте разберем, что нужно относить к ПДн:

1) Фамилия, имя, отчество, год, месяц, день и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы (Постановление по делу № А15- 2016/2009 от 05.10.2010. Президиум ВАС РФ, Постановление по делу № А36-5713/2014 от 29.04.2015. 19-й ААС).

2) Паспортные данные (см., например, Апелляционное определение Московского городского суда от 22.05.2014 № 33-14709).

3) Специальные категории: расовая, национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимной жизни.

4) Биометрические - физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта.

Применительно к отнесению данных к персональным важно понимать:

1) Никакой проверки или подтверждения, что данные относятся к конкретному физическому лицу, не требуется (закон такой процедуры не предусматривает). Поэтому оператор по факту не знает вымышленные ли это данные или нет, но от обязанностей по защите ПДн это не избавляет.

2) Персональными данными являются только те, которые могут идентифицировать физическое лицо (см., например, определение Санкт-Петербургского городского суда от 26 марта 2013 г. № 33-3815/13, Апелляционное определение Московского городского суда от 28 января 2014 г. N 33-5461/14).

В крайнем случае, спрашивайте у представителей Роскомнадзора!!!

Защита персональных данных при их обработке в Мастерской

Разделим все требования для простоты на четыре основные группы. Приступая к работе с персональными данными, вы должны:

1	Подготовить и принять пакет организационно-распорядительной документации (ОРД). Ознакомить персонал с принятыми ОРД.
2	Привести процессы работы с персональными данными в соответствие с законом. Обучить персонал. Направить «Уведомление» в Роскомнадзор.
3	Реализовать техническую защиту персональных данных в информационных системах и провести самостоятельную Оценку эффективности принимаемых мер по обеспечению безопасности персональных данных. Оценка эффективности возможна в форме «Аттестации».
4	Хранить базы с персональными данными на территории Российской Федерации.

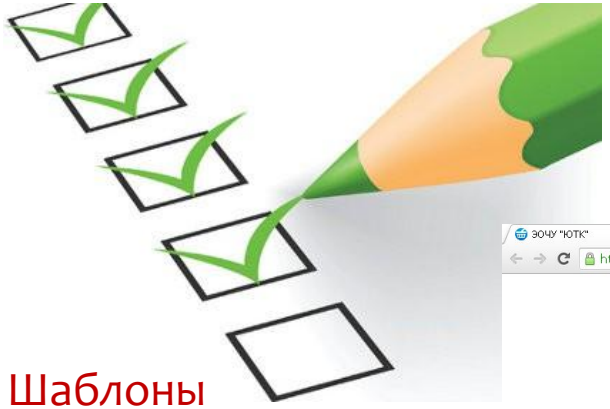
Требования по подготовке внутренних ОРД

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

Практика реализации этих мер сформировала необходимый минимум документов, который должен быть принят оператором, это:

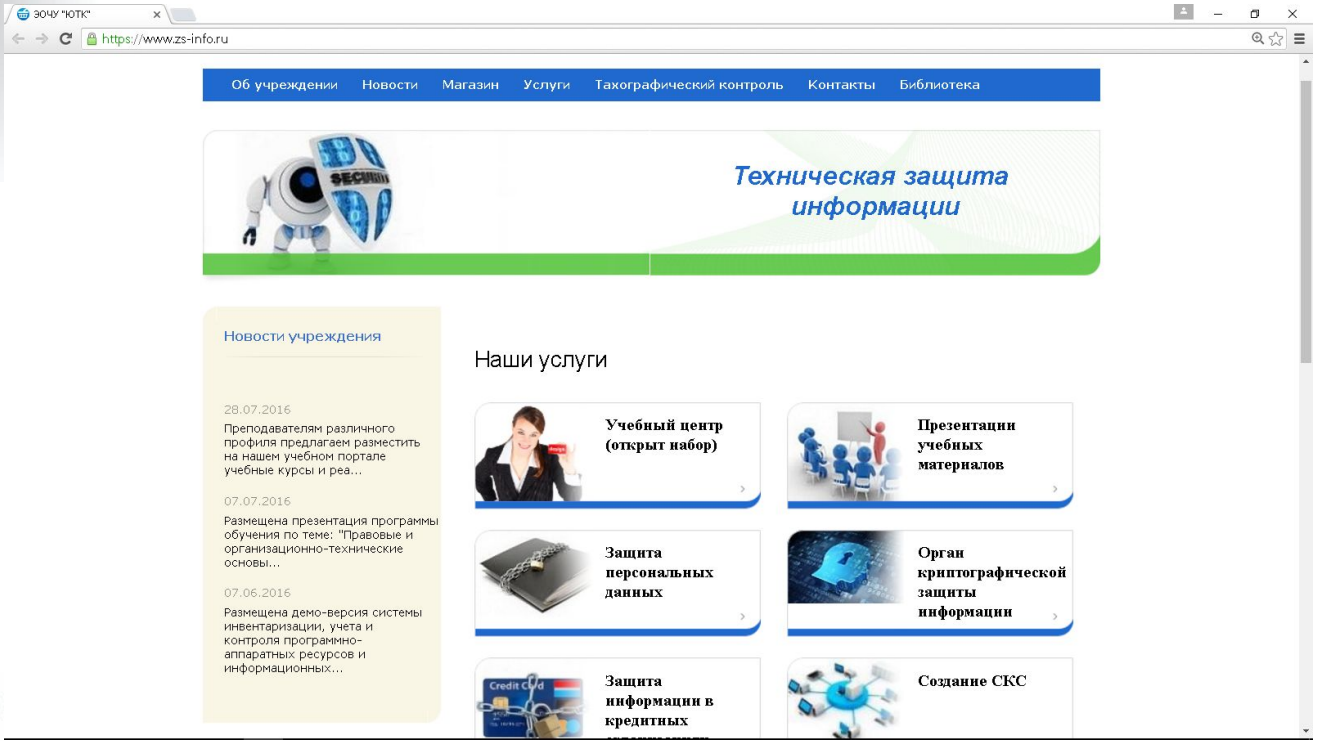
- общий документ, определяющий политику оператора в отношении обработки персональных данных;
- локальный акт или несколько актов, которые могут включать в себя описание всех процессов обработки персональных данных, включая перечень лиц, имеющих доступ к персональным данным, порядок обеспечения доступа и работы с персональными данными, процесс уничтожения персональных данных. Указанные акты также должны содержать конкретное описание правовых, организационных и технических мер защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
- локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

Предлагаем возможное Решение по подготовке ОРД

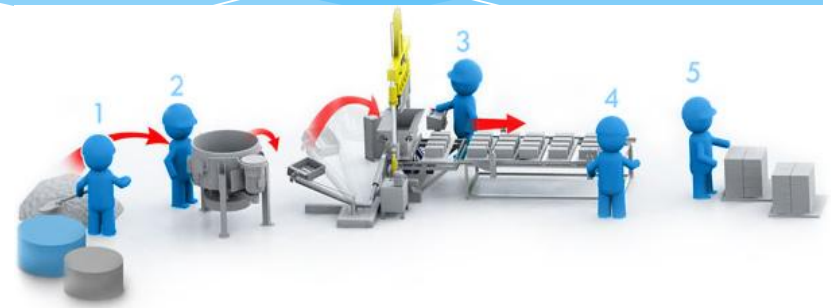


Основной комплект проектов документов по организации обработки и защите персональных данных доступен для скачивания в разделе защита персональных данных на сайте zs-info.ru

Шаблоны документов по персональным данным можно найти и в Интернете



Требования по приведению процессов обработки ПДн



Требования по приведению процессов работы с персональными данными в соответствие с законом

Персональные данные необходимо правильно собирать, обрабатывать и передавать.

Со всеми физическими лицами, у которых вы собираете персональные данные (например, через сайт клиента), должен быть заключен договор или взято согласие на их обработку.

С каждым контрагентом, которому вы передаете, предоставляете в доступ (например, другому оператору на субподряд) или от которого получаете персональные данные, необходимо заключить соглашение о поручении на их обработку.

Все сотрудники должны под роспись ознакомиться с внутренними документами организации по обработке и защите персональных данных и подписать обязательство о неразглашении.

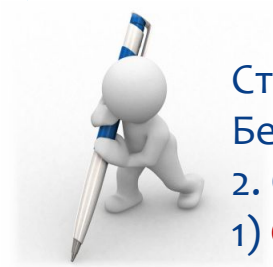
В Роскомнадзор должно быть подано уведомление об обработке персональных данных.

Требования по технической защите персональных данных в ИС. Определение уровня защищенности

Персональные данные
хранятся или как-то иначе обрабатываются в ИС - информационных системах , нужно определить уровень их защищенности, составив соответствующий акт, опираясь на Таблицу. **Это можно сделать самостоятельно**

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип (НДВ в СисПО)	2 тип (НДВ в ПрикПО)	3 тип (нет НДВ)
Специальные	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Любое	УЗ 1	УЗ 2	УЗ 3
Биометрические	Любых	Любое	УЗ 1	УЗ 2	УЗ 3
Иные	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 1	УЗ 3	УЗ 4
Общедоступные	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 2	УЗ 3	УЗ 4

Требования по технической защите персональных данных в ИС. Модель угроз и нарушителя



Статья 19. Меры по обеспечению
Безопасности персональных данных при их обработке
2. Обеспечение безопасности персональных данных достигается, в частности:
1) **Определением угроз безопасности** персональных данных при их обработке в информационных системах персональных данных;

Методические документы для разработки	
1	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Заместителем директора ФСТЭК России 15 февраля 2008 г.)
2	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Заместителем директора ФСТЭК России 14 февраля 2008 г.)
3	Методические рекомендации 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 (утв. Руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432)

Разработку частной модели угроз и нарушителя лучше поручить организации обладающей соответствующими лицензиями ФСТЭК России и ФСБ России

Уровень защищенности определен, что дальше?

От уровня защищенности персональных данных в ИСПДн зависит объем мероприятий по их защите и выбор сертифицированных средств защиты информации

Перечень минимальных мер защиты	1 УЗ	2 УЗ	3 УЗ	4 УЗ
Организовать режим обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих прав доступа в эти помещения	+	+	+	+
Обеспечить сохранность носителей ПДн	+	+	+	+
Утвердить перечень лиц, имеющих доступ к ПДн в рамках выполнения своих служебных обязанностей	+	+	+	+
Использовать сертифицированные СЗИ	+	+	+	+
Назначить приказом должностное лицо, ответственное за обеспечение безопасности ПДн в ИСПДн.	+	+	+	
Доступ к электронному журналу сообщении определить только лицам, которым необходимы сведения, содержащиеся в данном журнале для выполнения своих служебных обязанностей	+	+		
Обеспечить автоматическую регистрацию в электронном журнале безопасности изменения полномочии сотрудника по доступу к ПДн в ИСПДн	+			
Создать структурное подразделение ответственное за обеспечение безопасности ПДн в ИСПДн или возложить эти функции по обеспечению безопасности ПДн в ИСПДн на одно из существующих структурных подразделении	+			

Перечень минимальных мер защиты определен, что следующее?

Определение минимального класса защиты сертифицированных средств защиты информации

	УЗ1		УЗ2		УЗ3			УЗ4
	АУ1, АУ2 или АУ3 с ССОП	АУ3 без подключения к ССОП	АУ1, АУ2 или АУ3 с ССОП	АУ3 без подключения к ССОП	АУ2	АУ3 с подключением к ССОП	АУ3 без подключения к ССОП	-
СВТ	5 класс СВТ		5 класс СВТ		5 класс СВ			6 класс СВТ
СОВ	4 класс СОВ и 4 НДВ		4 класс СОВ и 4 НДВ		4 класс СОВ и 4 НДВ	4 класс СОВ	5 класс СОВ	5 класс СОВ
САЗ	4 класс САЗ и 4 НДВ		4 класс САЗ и 4 НДВ		4 класс САЗ и 4 НДВ	4 класс САЗ	5 класс САЗ	5 класс САЗ
МЭ	3 класс МЭ и 4 НДВ	4 класс МЭ и 4 НДВ	3 класс МЭ и 4 НДВ	4 класс МЭ и 4 НДВ	3 класс МЭ и 4 НДВ	3 класс МЭ	4 класс МЭ	5 класс МЭ
Другие СЗИ	Любое ТУ или 3Б и 4 НДВ		Любое ТУ или 3Б и 4 НДВ		Любое ТУ или 3Б и 4 НДВ	Любое ТУ или 3Б		Любое ТУ или 3Б

УЗ - уровень защищенности ИСПДн	**АУ -максимальный тип актуальных угроз**	**ССОП - сеть связи общего пользования (Интернет)**
СВТ - средство вычислительной техники	**СОВ - средство обнаружения вторжении**	**МЭ - межсетевое экранирование**
	САЗ - средство антивирусной защиты	

Уровень защищенности ПДн	**4 УЗ**	**3 УЗ**		**2 УЗ**			**1 УЗ**	
Тип актуальных угроз	3	2	3	1	2	3	1	2
Минимальный класс СКЗИ	КС1	КВ	КС1	КА	КВ	КС1	КА	КВ

Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных

После того, как Вы успешно разработали и внедрили проект системы защиты*, приступайте к **Оценке эффективности** принимаемых мер по обеспечению безопасности персональных данных.

Оценка эффективности может проводиться в формах добровольной аттестации по требованиям безопасности информации в системе сертификации ФСТЭК России, а также в других формах, выбираемых оператором ПДн (например, формах приемо-сдаточных испытаний СЗПДн, совместной оценки комиссией, состоящей из представителей Разработчика и Заказчика СЗПДн, и т. д.).

**Разработкой, внедрением и оценкой эффективности может заняться сама Мастерская или подрядчик, имеющий соответствующую лицензию ФСТЭК России, ФСБ России*

Поддержание достигнутого уровня защищенности при эксплуатации ИСПДн

Документ, подтверждающий соответствие

Вашей ИСПДн требованиям действующего законодательства по защите персональных данных, действителен в течение не более 3 лет, при условии обеспечения:

- неизменности состава системного и прикладного программного обеспечения ИСПДн;
- неизменности состава, конструкции, конфигурации и размещения средств вычислительной техники в ИСПДн;
- целостности, состава (комплектности) продукции, используемой в целях защиты информации, параметров её установки и настройки;
- допуска к обработке ПДн лиц, оформленных в установленном порядке;
- неизменности характеристик систем (электропитания, заземления, сигнализации) обеспечения эксплуатации объекта информатизации.

Эксплуатация ИСПДн предполагает выполнение обязательных мероприятий по нескольким видам контроля, ведению журналов регистрации, администрированию и т.д.

Требования по хранению баз персональных данных на территории Российской Федерации

С 1 сентября 2015 года
сбор и хранение персональных данных граждан Российской Федерации может происходить только на территории Российской Федерации. О месторасположении баз данных необходимо уведомить Роскомнадзор. Особенно это касается иностранных и российских компаний, чьи информационные системы полностью или частично располагаются за пределами РФ.

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор **обязан обеспечить** запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации

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

А(И)С© доступна для ознакомления
www.zs-info.ru

- Разработка и ведение организационно-распорядительной и эксплуатационно-технической документации.
- Обеспечение готовности и самооценка эффективности принимаемых мер по обеспечению безопасности персональных данных 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.

ЭКСПЕРТНО ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ
«ЮЖНАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ»

СПАСИБО ЗА ВНИМАНИЕ

Адрес нашего сайта с контактной информацией
и демоверсией сервиса А(И)С©:
www.zs-info.ru