Приложение №1
к Приказу директора
МБУ «Память» НГО
от 23.11 № 09-ТД

РЕГЛАМЕНТ

определение уровня защищенности персональных данных

Для определения уровня защищенности необходимо установить категории обрабатываемых персональных данных субъектов (физических лиц), вид обработки по форме отношений между субъектами и организацией, количество субъектов, а также тип угроз актуальных для информационной системы.

Категории обрабатываемых персональных данных (ПДн), подразделяются на 4 группы:

1 группа — **специальные категории ПДн**, к которым относятся информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информацию о здоровье и интимной жизни субъекта;

2 группа — **биометрические ПДн**, то есть данные, характеризующие биологические или физиологические особенности субъекта и используемые для установления личности, например, фотография или отпечатки пальцев;

3 группа — **общедоступные ПДн**, то есть сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом;

4 группа — **иные категории ПДн**, не представленные в трех предыдущих группах.

По форме отношений между организацией и субъектами обработка подразделяется на 2 вида:

- обработка персональных данных работников (субъектов, с которыми организация связана трудовыми отношениями);
- обработка персональных данных субъектов, не являющихся работниками организации.

По количеству субъектов, ПДн которых обрабатываются, нормативным актом определены лишь 2 категории:

- менее 100 000 субъектов;
- более 100 000 субъектов;

Типы актуальных угроз:

- угрозы 1-го типа связанны с наличием недекларированных (недокументированных) возможностей в системном ПО, используемом в ИСПДн;
- угрозы 2-го типа связанны с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн;
- угрозы 3-го типа не связаны с наличием недекларированных возможностей в программном обеспечении, используемом в ИСПДн.

Таблица уровней защищенности персональных данных

Категории ПДн		Специальные			Биометрические		Иные		Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	менее 100 тыс.			более 100 тыс.	менее 100 тыс.		более 100 тыс.	менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

Классификация персональных данных в контексте установления уровня защищенности ИСПДн

Установление **категории ПДн** подразделяемые на группы:

1. Первая категория включает специальные ПДн. Сюда относятся, прежде всего, данные о сексуальной ориентации и партнерах, состоянии здоровья, принадлежности к определенной расе или вероисповеданию, а также философские и политические взгляды.
2. Ко второй категории относятся биометрические персональные данные, позволяющие идентифицировать человека по особенностям его физиологии, например, отпечатку пальцев, рисунку сетчатки глаза, фотографии и т.д. Чтобы пользоваться такими ПДн легально, необходимо предварительно получить письменное согласие субъекта (кроме ситуаций, когда дело касается вопросов национальной безопасности, судебного производства или расследования преступлений).
3. Третья категория представлена общедоступной информацией о гражданине, которую он сам предоставляет для обработки. Речь идет о дате рождения, Ф.И.О.,

адресе, телефоне, образовании, профессии и других сведениях, опубликованных на страничках социальных сетей, в справочниках и т.д.

4. В четвертую категорию входят те личные сведения, которые нельзя включить ни в оду из других групп.

Определение **типа ПДн** осуществляется отдельно для каждой **ИСПДн** организации с учетом ее характеристик.

На показатель, кроме категории обрабатываемых личных сведений граждан, влияют и другие параметры:

1. Форма взаимоотношений между оператором и владельцами ПДн. Информационная система может предполагать обработку данных персонала организации или ИП (имеются ввиду как штатные, так и внештатные сотрудники, с которыми подписаны контракты) либо использовать сведения субъектов, не связанных с организацией трудовым договором.
2. Типы актуальных УБ. В расчет берутся не все существующие угрозы, а только те, которые можно реализовать в рамках конкретной ИС. Выделяют угрозы 1, 2 и 3 типа. Первый связан с НДВ в системном программном обеспечении, второй — с недекларируемыми возможностями прикладного софта, а третий — вообще не имеет отношения к НДВ используемого ПО.
3. Количество субъектов, личные данные которых копируются, обновляются, распространяются, блокируются и удаляются. Действующее законодательство предусматривает разделение на ИСПДн, обрабатывающие информацию менее 100 тысяч или более 100 тысяч граждан.

Уровни обозначаются УЗ1, УЗ2, УЗ3 и УЗ4, при этом самым высоким (то есть требующим наиболее серьезной защиты) является первый, а самым низким — четвертый.

Чтобы определить **1, 2, 3 или 4 уровень защищенности ИСПДн**, можно воспользоваться **таблицей** либо специальным онлайн-калькулятором, который есть на сайте ФСТЭК. Вам потребуется указать тип актуальных угроз, категорию ПДн, количество субъектов и взаимоотношения с ними (являются они вашими сотрудниками или нет), после чего программа сама рассчитает показатель. Но есть важный нюанс. Если неверно установить какой-либо из исходных параметров, например, преуменьшить или преувеличить тип УБ, то класс будет установлен неправильно. Избежать этого возможно при помощи привлечения экспертов в области информационной безопасности, которые грамотно выполнят за вас данную работу. Наиболее актуален подход, при котором обязанности по определению угроз и интеграции средств защиты

на возлагаются на профессионалов. Так удастся в короткие сроки привести систему в соответствие ФЗ-152, требованиям ФСТЭК и ФСБ (если нужно) и исключить штрафные санкции в будущем.

Важность правильного определения уровня защищенности ИСПДн

На основании проделанной работы по установлению степени защиты на каждую из ИС составляется акт классификации и формируется список требований, которые предстоит соблюдать при совершении различных операций с ПДн. Чем выше уровень, тем более продуманной и многоаспектной должна быть система защиты, а это напрямую влияет на сумму, которую придется потратить владельцам организации. Поэтому завышать УЗ нет никакого смысла, но и занижать тоже, иначе могут быть наложены санкции контролирующих органов.

Законодательные требования к ИСПДн с разным уровнем защищенности

Выбор, внедрение мер и средств нейтрализации угроз базируется на требованиях правительственного постановления 2012 года и Приказа ФСТЭК № 21 от 18 февраля 2013 года. Именно в последнем документе четко прописано, что нужно обеспечить для ИСПДн с 4, 3, 2 и 1 уровнем защищенности. Приведем пример того, что понадобится организациям с третьим классом ИС:

- утверждение внутренним приказом перечня лиц, имеющих доступ к ПДн;
- назначение сотрудника, который несет личную ответственность за соблюдением мер безопасности в отношении ИСПДн;
- подбор и интеграция СЗИ;
- применение сертифицированных средств защиты;
- установка замков, сигнализации, охраны в помещении, где располагается ИСПДн;
- разработка и утверждение правил доступа к данным при обычном режиме работы организации и во время внештатных ситуаций;
- хранение материальных носителей в сейфах с обязательным учетом их количества, характеристик, перечня лиц, имеющих доступ;
- обеспечение защиты средств виртуализации, ТС, систем связи и передачи ПДн;
- контроль работоспособности системы, фиксация происшествий;
- оценка эффективности и контроль выполнения нормативов ФСТЭК минимум раз в три года;
- внедрение средств аутентификации и идентификации для контроля доступа.

В зависимости от уровня защищенности ПДн определяется перечень требований, выполнение которых необходимо для нейтрализации угроз безопасности персональных данных.