Нормативно-правовые акты в области защиты персональных данных

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Главный закон об информации в России. Он определяет ключевые термины. Именно на этот закон и эти определения нужно ссылаться при составлении документов по информационной безопасности. В нем говорится, какая информация считается конфиденциальной, а какая — общедоступной, когда и как можно ограничивать доступ к информации, как происходит обмен данными. Также именно здесь прописаны основные требования к защите информации и ответственность за нарушения при работе с ней.

Ключевые моменты:

- нельзя собирать и распространять информацию о жизни человека без его согласия;
- тот, кто обрабатывает информацию, обязан ее защищать.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Этот закон регулирует работу с персональными данными — личными данными конкретных людей. Его обязаны соблюдать те, кто собирает, обрабатывает (получает, передает и хранит) эти данные

Ключевые моменты:

- если вы обрабатываете персональные данные, то обязаны держать их в секрете и защищать от посторонних;
- для защиты информации закон обязывает собирать персональные данные только с конкретной целью.

Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Этот нормативно-правовой акт устанавливает требования к защите персональных данных при их обработке в ИСПДн, а также уровни защищенности таких данных.

Ключевые моменты:

- договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе;
- оператору или лицу, осуществляющему обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора, необходимо создать систему защиты персональных данных, обеспечивающую безопасность персональных данных, включающую организационные и технические меры, которые определяются с учетом актуальных угроз безопасности и информационных технологий, используемых в ИСПДн;
- оператору (уполномоченному лицу) необходимо не реже 1 раза в 3 года организовывать и проводить контроль за выполнением указанных требований (самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации;

Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

- необходимо определить угрозы какого типа из трех возможных актуальны для этих ИСПДн;
- необходимо разработать документ, на основании которого можно оценить возможный вред субъектам персональных данных;
- необходимо установить количество субъектов, персональные данные которых обрабатываются в каждой ИСПДн;
- необходимо определить какой уровень защищенности персональных данных из четырех возможных необходимо обеспечивать при их обработке в ИСПДн;
- необходимо выполнить требования предусмотренные в ПП-1119, для обеспечения соответствующего уровня защищенности персональных данных.

Тип ИСПДн	ПДн только сотрудников оператора	Количество субъектов ПДн	Требуемый уровень если актуальны угрозы		
			1 типа	2 типа	3 типа
ИСПДн-С Специальные	Нет	> 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100 000	УЗ-1	УЗ-2	УЗ-3
	Да	Любое	УЗ-1	УЗ-2	УЗ-3
ИСПДн-Б Биометрические	Да/Нет	Любое	УЗ-1	УЗ-2	УЗ-3
ИСПДн-И Иные	Нет	> 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да	Любое	УЗ-2	УЗ-3	УЗ-4
ИСПДн-О Общедоступные	Нет	> 100 000	УЗ-2	УЗ-2	УЗ-4
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да	Любое	УЗ-2	УЗ-3	УЗ-4

Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

В данном документе подробно рассматривается содержание необходимых мер в зависимости от установленного уровня защищенности обрабатываемых персональных данных

В качестве пособия по реализации необходимых мер защиты персональных данных можно использовать Методический документ ФСТЭК России от 18.02.2013 «Меры защиты информации в государственных информационных системах», поскольку большинство мер между собой схожи.

Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении 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»

В документе рассматриваются отдельные требования к организации работы со средствами криптографической защиты информации (далее – СКЗИ). Данные требования обязательны к исполнению наравне с требованиями Постановления правительства РФ от 01.11.2012 № 1119 и Приказа ФСТЭК России от 18.02.2013 г. № 21 поскольку персональные данные необходимо защищать в том числе с применением криптографических средств

Ключевые моменты:

- должен быть назначен орган криптографической защиты информации либо сотрудники, выполняющие его функции;
- должно быть организовано обучение сотрудников работе с СКЗИ;
- должен быть организован порядок работы пользователей с СКЗИ и доступ к данным средствам.

Иная нормативная документация в области защиты ПДн

1. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ;
2. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ;
3. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ;
4. Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ;
5. Постановление Правительства Российской Федерации от 29.12.2022 № 2526;
6. Постановление Правительства Российской Федерации от 10.01.2023 № 6;
7. Постановление Правительства Российской Федерации от 16.01.2023 № 24;
8. Приказ ФСБ России от 10.07.2014 № 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».

Иная нормативная документация в области защиты ПДн

9. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных»
10. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»
11. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных»
12. Постановление Правительства Российской Федерации от 29.06.2021 № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных»
13. Постановление Правительства РФ от 21.03.2012 № 211 (ред. от 15.04.2019) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»