Рекомендации по внедрению организационных
(административных) мер защиты
персональных данных

Рекомендации по внедрению организационных (административных) мер защиты персональных данных разработаны для <организации> (далее – Оператор).

Рекомендации разработаны в соответствии с Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1. Общие рекомендации

1.1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

1.2. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством и иными нормативными правовыми актами РФ в области персональных данных.

1.3. Оператор может привлекать к решению задач по приведению обработки и защиты персональных данных в соответствие требованиям законодательства специализированные организации, имеющие разрешение (лицензию) на осуществление деятельности по технической защите конфиденциальной информации.

2. Организационные меры защиты

2.1. Оператор назначает лицо, ответственное за организацию обработки персональных данных.

2.2. Оператор разрабатывает и внедряет документы, определяющие политику оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

2.3. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

2.4. Оператор определяет перечень персональных данных, подлежащих обработке, с указанием целей и оснований их обработки, перечень информационных систем и помещений, в которых может осуществляться обработка персональных данных, а также перечень лиц, доступ которых к персональным данным необходим для выполнения ими служебных (трудовых) обязанностей.

2.5. Оператор устанавливает правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в информационных системах персональных данных.

2.6. Оператор организует контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

2.7. Оператор организует обнаружение фактов несанкционированного доступа к персональным данным и принимает адекватные меры по недопущению их повторения.

2.8. Оператор обеспечивает учет и сохранность носителей персональных данных.

2.9. Оператор организует систему резервирования и восстановления персональных данных, которые могут быть модифицированы или уничтожены вследствие несанкционированного доступа.

2.10. Оператор осуществляет регистрацию обращений субъектов персональных данных с целью исполнения их законных прав.

2.11. Оператор проводит оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства, а также оценивает соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством.

2.12. Оператор определяет уровень защищенности персональных данных при их обработке в информационных системах персональных данных.

2.13. Оператор определяет перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2.14. Оператор осуществляет ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение работников.

3. Требования к защите помещений

3.1. Оператор организует режим обеспечения безопасности помещений, в которых осуществляется обработка персональных данных, а также размещены элементы информационных систем персональных данных, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

3.2. Указанные помещения должны быть оборудованы системами охранной и пожарной сигнализации.

3.3. Входы в указанные помещения должны быть оборудованы запираемыми прочными дверьми.

3.4. Система охранного видеонаблюдения должна быть настроена таким образом, чтобы входы в указанные помещения контролировались и фиксировались службой обеспечения безопасности (правопорядка).