Сведения о реализуемых требованиях к защите персональных данных в ООО «КЕСКО-Балтия»

1. Защита персональных данных, обрабатываемых в ООО «КЕСКО-Балтия» (далее – Оператор) обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований законодательства в области защиты персональных данных.

2. Правовые меры включают в себя:

• разработку локальных актов Оператора, реализующих требования российского законодательства, в том числе Политики в отношении обработки персональных данных, и размещение ее на интернет-сайте Оператора;

• реализацию требований о соблюдении конфиденциальности персональных данных;

• реализацию требований об обеспечении реализации субъектом персональных данных своих прав, включая право на доступ к информации;

• реализацию требований к защите 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;

• реализацию иных требований законодательства Российской Федерации;

• отказ от любых способов обработки персональных данных, не соответствующих целям, заранее предопределенным Оператором.

3. Организационные меры включают в себя:

• назначение лица, ответственного за организацию обработки персональных данных;

• назначение лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее - ИСПДн);

• определение перечня должностей работников и третьих лиц, допущенных к обработке персональных данных, имеющих доступ к персональным данным;

• определение перечня помещений, где ведется обработка персональных данных. Ограничение допуска посторонних лиц в помещения Оператора, недопущение их нахождения в помещениях, где ведется работа с персональными данными и размещаются технические средства их обработки, без контроля со стороны работников Оператора;

• ознакомление работников Оператора с положениями законодательства Российской Федерации в области персональных данных, в том числе с требованиями

к защите персональных данных, с локальными актами Оператора по вопросам обработки персональных данных;

• определение в трудовых обязанностях и должностных инструкциях работников Оператора обязанностей по обеспечению безопасности обработки персональных данных и ответственности за нарушение установленного порядка;

• регламентацию процессов обработки персональных данных;

• организацию учёта материальных носителей персональных данных и их хранения, обеспечивающих предотвращение хищения, подмены, несанкционированного копирования и уничтожения;

• определение угроз безопасности персональных данных при их обработке в ИСПДн, формирование на их основе моделей угроз;

• размещение технических средств обработки персональных данных в пределах охраняемой территории;

• определение перечня ИСПДн;

• определение типа угроз безопасности персональных данных, актуальных для информационных систем персональных данных с учетом оценки возможного вреда субъектам персональных данных, который может быть причинен в случае нарушения требований безопасности, определение уровня защищенности персональных данных и реализацию требований к защите персональных данных при их обработке в информационных системах, исполнение которых обеспечивает установленные уровни защищенности персональных данных.

4. Технические меры включают в себя:

• разработку на основе модели угроз системы защиты персональных данных для установленных Правительством Российской Федерации уровней защищенности персональных данных при их обработке в ИСПДн;

• использование для нейтрализации актуальных угроз средств защиты информации, прошедших процедуру оценки соответствия;

• оценку эффективности принимаемых мер по обеспечению безопасности персональных данных;

• реализацию системы разграничения доступа работников к информации, содержащей персональные данные, обрабатываемой в ИСПДн, и программно-аппаратным, и программным средствам защиты информации;

• регистрацию и учёт действий с персональными данными пользователей ИСПДн, где обрабатываются персональные данные;

• выявление вредоносного программного обеспечения (применение антивирусных программ) на всех узлах информационной сети Оператора, обеспечивающих соответствующую техническую возможность;

• безопасное межсетевое взаимодействие (применение межсетевого экранирования);

• передача информации с использованием информационно-телекоммуникационных сетей осуществляется при помощи средств криптографической защиты информации;

• обнаружение вторжений в ИСПДн Оператора, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

• регулярное резервное копирование информации и баз данных, содержащих персональные данные субъектов персональных данных;

• периодическое проведение мониторинга действий пользователей, разбирательств по фактам нарушения требований безопасности персональных данных;

• регулярные проверки соответствия системы защиты персональных данных, аудит уровня защищенности персональных данных в ИСПДн, функционирования средств защиты информации, выявления изменений в режиме обработки и защиты персональных данных.