

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия условий обработки персональных данных и принимаемых мер по их защите требованиям, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами и правовыми актами Департамента.

1.2. Внутренний контроль процесса обработки и обеспечения безопасности персональных данных заключается в проверке выполнения установленных законодательством Российской Федерации и правовыми актами Департамента требований к процессам обработки (в том числе хранения) персональных данных и соблюдения требований по обеспечению безопасности персональных данных при их обработке. Целью проведения внутренних проверок является выявление и своевременное устранение нарушений правил обработки персональных данных и требований по обеспечению безопасности персональных данных, в том числе путем принятия дополнительных мер по обеспечению безопасности персональных данных.

1.3. Мероприятия по осуществлению внутреннего контроля процесса обработки и обеспечения безопасности персональных данных направлены на решение следующих задач:

обеспечение соблюдения государственными гражданскими служащими Ивановской области, замещающими должности государственной гражданской службы Ивановской области в Департаменте, и работниками, замещающими должности, не являющиеся должностями государственной гражданской службы в Департаменте (далее - сотрудники) требований нормативных правовых актов, правовых актов Департамента, регулирующих сферу обработки персональных данных;

оценка компетентности сотрудников, участвующих в процессе обработки и (или) обеспечения безопасности персональных данных, и определение

необходимости их обучения по вопросам обработки персональных данных и (или) обеспечения безопасности персональных данных;

обеспечение соответствия условий эксплуатации технических средств, участвующих в обработке персональных данных, и средств защиты информации требованиям технической и эксплуатационной документации;

выявление изменений технологического процесса обработки персональных данных, новых угроз безопасности персональных данных и их источников, иных факторов, влияющих на оценку угроз безопасности персональных данных, обрабатываемых в Департаменте;

сбор информации, необходимой для анализа выявленных нарушений требований по обработке (в том числе хранению) и обеспечению безопасности персональных данных, выработки предложений и принятия решений по совершенствованию порядка обработки и обеспечения безопасности персональных данных.

2. Формы проведения внутреннего контроля процесса обработки и обеспечения безопасности персональных данных

2.1. Внутренний контроль процесса обработки и обеспечения безопасности персональных данных проводится в следующих формах:

текущий контроль;

комплексные проверки.

2.2. Текущий контроль соблюдения правил обработки персональных данных и требований по обеспечению их безопасности осуществляется руководителями структурных подразделений Департамента, сотрудники которых участвуют в процессе обработки персональных данных; при осуществлении обработки персональных данных государственными гражданскими служащими Департамента, замещающими должности государственной гражданской службы, не входящие в состав структурных подразделений Департамента, текущий контроль осуществляется в порядке самоконтроля.

Текущий контроль направлен на обеспечение соблюдения:

порядка доступа в помещения, в которых установлены технические средства, участвующие в обработке персональных данных, либо хранятся материальные носители персональных данных;

правил эксплуатации технических средств, участвующих в обработке персональных данных, и правил работы с материальными носителями персональных данных, а также порядка доступа к ним;

порядка обращения с паролями (парольной информацией), материальными носителями аутентификационной и ключевой информации;

порядка реагирования на нештатные ситуации в целях недопущения их игнорирования;

установленных Правил обработки персональных данных в Департаменте.

Текущий контроль осуществляется на постоянной основе. Лица, осуществляющие текущий контроль соблюдения правил обработки персональных данных и требований по обеспечению их безопасности, самостоятельно обеспечивают соблюдение установленных правил и требований, а в случае серьезного или неоднократного нарушения сотрудником установленных правил и требований – незамедлительно руководителю Департамента.

2.3. Комплексные проверки условий обработки персональных данных и принимаемых мер по их защите установленным требованиям проводятся не реже чем 1 раз в год создаваемой в соответствующих целях на основании распоряжения Департамента комиссией.

Комплексные проверки направлены на:

выявление фактов обработки персональных данных, не регламентированных распоряжениями Департамента;

выявление изменений технологического процесса обработки персональных данных, новых угроз безопасности персональных данных и их источников, иных факторов, влияющих на оценку угроз безопасности персональных данных, обрабатываемых в Департаменте;

оценку актуальности документов, регламентирующих порядок обработки персональных данных в Департаменте, доступ к ним и необходимость их корректировки;

оценку соответствия принятых мер по обеспечению безопасности персональных данных в Департаменте требованиям законодательства Российской Федерации;

обеспечение соблюдения условий эксплуатации средств защиты информации, предусмотренных технической и эксплуатационной документацией.

Одновременно при проведении комплексной проверки осуществляется проверка соблюдения Порядка доступа государственных гражданских служащих Ивановской области, замещающих должности государственной гражданской службы Ивановской области в Департаменте, и работников, замещающих должности, не являющиеся должностями государственной гражданской службы в Департаменте, в помещения, в которых ведется обработка персональных данных.

2.4. По результатам комплексной проверки условий обработки персональных данных комиссия совместно с лицом, ответственным за

организацию обработки персональных данных в Департаменте (в случае если лицо, ответственное за организацию обработки персональных данных в Департаменте, не было включено в состав комиссии) разрабатывает комплекс мер, направленных на устранение нарушений в сфере персональных данных.