

2.1.4. актуальность информации в приказе «О назначении ответственных лиц за обеспечение безопасности персональных данных при их обработке»;

2.1.5. наличие и актуальность документа, определяющего политику Учреждения в отношении обработки персональных данных;

2.1.6. наличие и актуальное состояние оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства;

2.1.7. наличие документов, подтверждающих факт ознакомления работников с законодательством Российской Федерации и локальными актами Учреждения, регулирующими обработку и защиту персональных данных;

2.1.8. проверка соответствия локальных актов Учреждения законодательству Российской Федерации о персональных данных на дату проведения внутреннего контроля и (или) аудита;

2.1.9. проверка законности обработки отдельных категорий персональных данных (специальные, биометрические) и их соответствия целям обработки.

2.2. Тематика проверок обработки персональных данных с использованием средств автоматизации:

2.2.1.соответствие полномочий пользователя матрице доступа;

2.2.2.соблюдение пользователями информационных систем персональных данных Учреждения парольной политики;

2.2.3.соблюдение пользователями информационных систем персональных данных антивирусной политики;

2.2.4.соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных;

2.2.5.соблюдение порядка доступа в помещения Учреждения, в которых ведется обработка персональных данных с помощью средств автоматизации;

2.2.6.соблюдение порядка работы со средствами защиты информации;

2.2.7.знание пользователями информационных систем персональных данных о своих действиях в нештатных ситуациях.

2.3.Тематика проверок обработки персональных данных без использования средств автоматизации:

2.3.1.обеспечение надлежащего хранения бумажных носителей, содержащих персональные данные;

2.3.2.соблюдение порядка доступа к бумажным носителям, содержащим персональные данные;

2.3.3.соблюдение порядка доступа в помещения, где обрабатываются и хранятся бумажные носители, содержащие персональные данные;

2.3.4.соблюдение правил обработки персональных данных, осуществляемой без использования средств автоматизации.

3. Порядок проведения проверок

3.1.Проверки осуществляются ответственным за организацию обработки персональных данных (далее по тексту – Ответственный) либо комиссией непосредственно в месте(ах) обработки персональных данных путем опроса работников, участвующих в процессе обработки персональных данных, при необходимости, осмотра рабочих мест работников, мест хранения носителей, содержащих персональные данные, документов, баз данных и т.п.

3.2.Ответственный (комиссия) имеет право:

- запрашивать у сотрудников организации необходимую информацию;

- требовать от уполномоченных на обработку персональных данных лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить Директору Учреждения предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить Директору Учреждения предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

3.3. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне исследованы и (или) установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;

эффективность принимаемых мер по обеспечению безопасности персональных данных;

- состояние учета машинных носителей персональных данных;

соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

осуществление мероприятий по обеспечению целостности персональных данных.

3.4. В отношении персональных данных, ставших известными Ответственному (членам комиссии) в ходе проведения внутреннего контроля и (или) аудита, должна быть обеспечена конфиденциальность.

3.5.По окончанию каждой проверки составляется отчет, содержащий результаты проведенной проверки. Форма отчета приведена в приложении к настоящим Правилам.

3.6.При выявлении в ходе проверки нарушений в отчете делается запись о мерах, которые необходимо принять для устранения выявленных нарушений и сроках исполнения.

3.7.Отчет предоставляется директору Учреждения. После устранения всех нарушений Ответственным составляется об этом акт.