

ПРАВИЛА **осуществления внутреннего контроля соответствия обработки** **персональных данных**

1. Общие положения

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в ФГБУ «СибНИГМИ» требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора (далее – Правила), определяют порядок действий, направленных на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в ФГБУ «СибНИГМИ», а также цели, основания и виды внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие Правила разработаны на основании:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановления Правительства от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановления Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. Целью осуществления внутреннего контроля соответствия обработки персональных данных в ФГБУ «СибНИГМИ» требованиям к защите персональных данных (далее – внутренний контроль) является соблюдение в организации законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных.

2. Тематика внутреннего контроля

2.1. Тематикой проверок обработки персональных данных с использованием средств автоматизации является:

- соблюдение пользователями информационных систем персональных данных (далее – ИСПД) оператора парольной защиты;
- соблюдение пользователями ИСПД в организации антивирусной защиты;
- соблюдение порядка доступа в помещения оператора, где расположены элементы ИСПД;
- соблюдение порядка работы со средствами защиты информации;
- знание пользователями информационных систем персональных данных о своих действиях во внештатных ситуациях;
- проверка своевременности исполнения запросов субъектов персональных данных;
- проверка автоматизированных рабочих мест пользователей на предмет наличия возможных вредоносных программ и запрещенных информационных ресурсов.

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

- хранение бумажных носителей с персональными данными;
- доступ к бумажным носителям с персональными данными;
- доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными;

3. Порядок проведения внутренних проверок

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в организации организуется проведение периодических проверок условий обработки персональных данных в соответствии с Планом внутренних проверок условий обработки персональных данных в организации, а также внеплановых проверок условий обработки персональных данных.

3.2. Проверки осуществляются ответственным за организацию обработки персональных данных лицом или лицами (далее – Ответственное лицо).

3.3. Внеплановые проверки проводятся в случае поступления оператору сведений об имеющихся нарушениях при осуществлении обработки персональных данных.

3.4. Проверки осуществляются ответственным лицом непосредственно на месте обработки персональных данных путем опроса сотрудников, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных, а также в иных формах в соответствии с действующим законодательством.

3.5. Для каждой проверки составляется Протокол проведения внутренней проверки условий обработки персональных данных в организации (далее – Протокол).

3.6. При выявлении в ходе проверки нарушений Ответственным лицом в Протоколе делается запись о необходимых мероприятиях по устранению выявленных нарушений и сроках их устранения.

3.7. Протоколы хранятся у Ответственного лица в течение текущего года. Уничтожение Протоколов обеспечивается Ответственным лицом самостоятельно в январе года, следующего за проверочным. При необходимости протоколы могут храниться до полного устранения нарушений.

3.8. О результатах проверки и мерах, необходимых для устранения нарушений, докладывается директору ФГБУ «СибНИГМИ» Ответственным лицом.

Исполнитель:

Специалист по кадрам Т.А.Пустовалова