

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(Минобрнауки России)



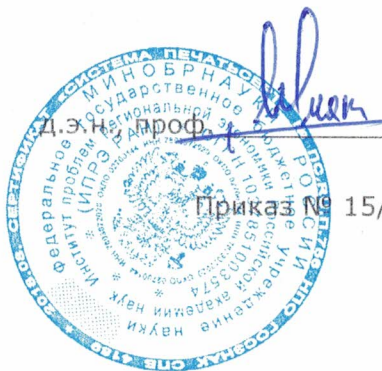
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ИНСТИТУТ ПРОБЛЕМ РЕГИОНАЛЬНОЙ ЭКОНОМИКИ РОССИЙСКОЙ АКАДЕМИИ НАУК

(ИПРЭ РАН)

УТВЕРЖДАЮ

Директор ИПРЭ РАН

А.Д. Шматко



Приказ № 15/2 от 04 марта 2024 г.
Приложение № 3

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

**Федерального государственного бюджетного учреждения науки
Институт проблем региональной экономики
Российской академии наук
(ИПРЭ РАН)**

Санкт-Петербург
2024 год

1. Общие положения

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в ИПРЭ РАН 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 ИПРЭ РАН, 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 ИПРЭ РАН требованиям к защите персональных данных (далее – внутренний контроль) является соблюдение в ИПРЭ РАН 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:

- соответствие полномочий пользователя матрице доступа;
- соблюдение пользователями информационных систем персональных данных (далее – ИСПД) оператора парольной политики;
- соблюдение пользователями ИСПД в организации антивирусной политики;
- соблюдение пользователями ИСПД оператора правил работы со съемными носителями персональных данных;
- соблюдение ответственными за криптографические средства защиты информации правил работы с ними;
- соблюдение порядка доступа в помещения оператора, где расположены элементы ИСПД;
- соблюдение порядка резервирования баз данных и хранения резервных копий;
- соблюдение порядка работы со средствами защиты информации;
- знание пользователями информационных систем персональных данных о своих действиях во внештатных ситуациях.

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

- хранение и доступ бумажных носителей 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 ИПРЭ РАН организуется проведение периодических и внеплановых проверок условий обработки персональных данных.

3.2. Проверки осуществляются ответственным за организацию обработки персональных данных лицом или лицами (далее – Ответственное лицо) либо комиссией, образуемой по указанию директора ИПРЭ РАН (далее – комиссия).

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

3.4. Проверки осуществляются ответственным лицом (комиссией) 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 (председателем комиссии) в Протоколе делается запись о необходимых мероприятиях по устранению выявленных нарушений и сроках их устранения.

3.7. Протоколы хранятся у Ответственного лица (председателя комиссии) в течение текущего года. Уничтожение Протоколов обеспечивается Ответственным лицом (комиссией) самостоятельно в январе года, следующего за проверочным.

3.8. О результатах проверки и мерах, необходимых для устранения нарушений, докладывается директору ИПРЭ РАН Ответственным лицом (председателем комиссии).