

**Правила**  
осуществления внутреннего контроля соответствия процедуры обработки персональных  
данных требованиям к защите персональных данных

1. Настоящие Правила осуществления внутреннего контроля соответствия процедуры обработки персональных данных требованиям к защите персональных данных, устанавливают порядок осуществления внутреннего контроля соответствия процедуры обработки персональных данных (далее – ПДн) требованиям к защите ПДн, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятым в соответствии с ним нормативным правовым актам и локальным актами государственного автономного учреждения дополнительного профессионального образования Иркутской области «Институт развития образования Иркутской области» (далее соответственно – ГАУ ДПО ИРО, Правила).

2. Осуществление внутреннего контроля соответствия процедуры обработки ПДн требованиям к защите ПДн в ГАУ ДПО ИРО осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», настоящими Правилами и другими нормативными правовыми актами, касающимися обработки ПДн.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных Федеральным законом № 152-ФЗ.

4. Целью осуществления внутреннего контроля соответствия процедуры обработки ПДн требованиям к защите ПДн (далее – внутренний контроль) является обеспечение защиты ПДн от несанкционированного доступа, неправомерного их использования или утраты, определение порядка и правил осуществления внутреннего контроля.

5. Внутренний контроль делится на текущий, плановый и внеплановый.

6. Текущий внутренний контроль осуществляется на постоянной основе работником, ответственным за организацию обработки ПДн, в ГАУ ДПО ИРО (далее – ответственный за организацию обработки) в ходе мероприятий по обработке ПДн.

7. Ответственный за организацию обработки имеет право:

1) запрашивать у работников ГАУ ДПО ИРО информацию, необходимую для реализации полномочий;

2) требовать от уполномоченных на обработку ПДн должностных лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем ПДн;

3) принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства Российской Федерации;

4) вносить ректору ГАУ ДПО ИРО предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПДн при их обработке;

5) вносить ректору ГАУ ДПО ИРО предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации о ПДн.

8. Плановый внутренний контроль осуществляется комиссией, образуемой приказом ГАУ ДПО ИРО, в состав которой входят работники ГАУ ДПО ИРО, допущенные к обработке ПДн (далее – комиссия).



9. Плановый внутренний контроль проводится на основании утвержденного ректором ГАУ ДПО ИРО Плана проведения внутренних проверок режима защиты персональных данных в ГАУ ДПО ИРО, разрабатываемого председателем комиссии, форма которого установлена Приложением № 1 к настоящим Правилам. Периодичность плановой проверки – не реже одного раза в год.

10. Внеплановый внутренний контроль может осуществляться на основании поступившего в ГАУ ДПО ИРО письменного заявления о нарушениях правил обработки ПДн (внеплановые проверки). Решение о проведении внеплановой проверки принимается ректором ГАУ ДПО ИРО на основании предложения председателя комиссии в течение 3 (трех) рабочих дней с момента поступления соответствующего заявления.

11. В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах.

12. При проведении внутреннего контроля ответственным за организацию обработки или комиссией должны быть полностью, объективно и всесторонне изучены:

- 1) наличие, учет, порядок хранения и обезличивания ПДн;
- 2) порядок и условия применения организационных и технических мер по обеспечению безопасности ПДн при их обработке;
- 3) порядок и условия применения средств защиты информации;
- 4) эффективность принимаемых мер по обеспечению безопасности ПДн;
- 5) состояние учёта ПЭВМ и съемных носителей информации, содержащей ПДн;
- 6) соблюдение правил доступа к ПДн;
- 7) наличие (отсутствие) фактов несанкционированного доступа к ПДн;
- 8) порядок проведения мероприятий и результаты по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 9) порядок проведения мероприятий по обеспечению целостности ПДн.

13. В отношении ПДн, ставших известными членам комиссии или ответственному за организацию обработки в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность ПДн.

14. Срок проведения плановой и внеплановой проверки не может составлять более 30 дней со дня принятия решения о её проведении.

12. Результаты внутреннего контроля оформляются в виде протокола проведения внутренней проверки (далее – протокол). Протокол проведения плановой, внеплановой проверки подписывается всеми членами комиссии.

13. Все мероприятия по осуществлению внутреннего контроля вносятся в журнал проведения внутренних проверок режима защиты персональных данных в ГАУ ДПО ИРО, форма которого установлена Приложением № 2 к настоящим Правилам.

14. При выявлении в ходе внутреннего контроля нарушений ответственным за организацию обработки либо председателем комиссии в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

15. Протоколы хранятся у ответственного за организацию обработки в течение текущего года. Уничтожение протоколов проводится ответственным за организацию обработки самостоятельно в январе года, следующего за проверочным годом.

16. О результатах внутреннего контроля и мерах, необходимых для устранения нарушений, ректору ГАУ ДПО ИРО докладывает ответственный за организацию обработки либо председатель комиссии.

Приложение № 1  
к Правилам осуществления внутреннего  
контроля соответствия процедуры  
обработки персональных данных  
требованиям к защите персональных  
данных

План  
проведения внутренних проверок режима защиты персональных данных  
в государственном автономном учреждении дополнительного  
профессионального образования Иркутской области  
«Институт развития образования Иркутской области»  
на 20\_\_ год

№ п/п	Мероприятие	Периодичность	Дата, подпись исполнителя
1.	Контроль соблюдения правил обработки персональных данных (далее – ПДн)	Ежемесячно	
2.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	Ежегодно	
3.	Контроль соблюдения режима парольной защиты	Ежемесячно	
4.	Контроль выполнения антивирусной защиты	Еженедельно	
5.	Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	
6.	Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИС	Еженедельно	
7.	Контроль над обеспечением резервного копирования	Ежемесячно	
8.	Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также анализ появления новых, еще неизвестных, угроз	Ежегодно	
9.	Поддержание в актуальном состоянии нормативно-организационных документов	Ежеквартально	
10.	Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное программное обеспечение, специально дорабатываемое собственными разработчиками или сторонними организациями (при наличии)	Ежемесячно	
11.	Тестирование всех функций СЗИ от НСД с помощью специальных программных средств	Ежегодно	

Приложение № 2

к Правилам осуществления внутреннего контроля  
соответствия обработки персональных данных  
требованиям к защите персональных данных

ЖУРНАЛ

проведения внутренних проверок режима защиты персональных данных в государственном автономном учреждении  
дополнительного профессионального образования Иркутской области  
«Институт развития образования Иркутской области»

Журнал начат « \_\_\_\_ » \_\_\_\_ 20 \_\_\_\_ г.

Должность \_\_\_\_\_ / \_\_\_\_\_ /  
подпись \_\_\_\_\_ ФИО

Журнал завершён « \_\_\_\_ » \_\_\_\_ 20 \_\_\_\_ г.

Должность \_\_\_\_\_ / \_\_\_\_\_ /  
подпись \_\_\_\_\_ ФИО

Журнал составлен на \_\_\_\_ листах



[illegible]