Приложение 4
УТВЕРЖДЕНЫ Приказом ГБОУ ДПО
«ДОНРИРО» от 29.12.2023 № 178

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в
ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ДОНЕЦКИЙ РЕСПУБЛИКАНСКИЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ»

1. Общие положения

1.1 Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ДОНЕЦКИЙ РЕСПУБЛИКАНСКИЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ» (далее - Правила, Институт) определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным законодательством Российской Федерации и принятыми в соответствии с ним нормативными правовыми актами.

1.2 Настоящие Правила разработаны в соответствии с:

1. Федеральным законом от 27 июня 2006 г. N 152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»);
2. Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
3. Постановлением Правительства Российской Федерации от 21 марта 2012 г. N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" и другими нормативными правовыми актами;
4. Постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке информационных системах персональных данных».

1.3 Настоящими Правилами в своей работе должны руководствоваться сотрудники Института, осуществляющие внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных.

2. Структура процессов по внутреннему контролю

2.1 Контроль выполнения требований по защите персональных данных в структурных подразделениях Института осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, а также выработки мер по их устранению и недопущению в дальнейшем.

2.2 Контроль выполнения требований по защите персональных данных в структурных подразделениях Института осуществляет ответственный за организацию обработки персональных данных в Институте и администратор информационной безопасности Института.

2.3 Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

2.4 Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

2.5 Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов персональных данных или нарушения требований по защите персональных данных.

2.6 Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений Института не позднее, чем за 24 часа до начала проверки.

2.7 Проверки по частным вопросам могут проводиться без уведомления руководителей структурных подразделений Института.

2.8 Периодичность и сроки проведения плановых проверок структурных подразделений Института устанавливаются планом проверок на календарный год. Сроки проведения плановых проверок доводятся руководителям проверяемых подразделений не позднее, чем за 10 суток до начала проверки.

3. Порядок подготовки к проверке

3.1 Общий контроль выполнения требований по обеспечению безопасности персональных данных в структурных подразделениях Института осуществляется в соответствии с Планом проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных Института, составляемым по форме, согласно приложению 1 и утвержденным ректором Института.

3.2 Ответственный за выполнение мероприятий по контролю исполнения структурными подразделениями Института требований документов по обеспечению безопасности персональных данных подготавливает предложения по составу комиссии или группы проверяющих лиц.

3.3 Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений Института информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения Института.

4. Порядок проведения проверки

4.1 Руководитель проверяемого структурного подразделения Института обязан оказывать содействие комиссии по проверке или группе проверяющих лиц и, в случае необходимости, определять должностное лицо, ответственное за сопровождение проверки.

4.2 Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

4.3 Должны быть согласованы конкретные вопросы по объему, содержанию, срокам проведения проверки, а также, каких сотрудников структурных подразделений Института необходимо привлечь к проверке и какие помещения следует посетить.

4.4 Общий порядок проведения проверки включает:

- выявление сотрудников, задействованных в обработке персональных данных;
- проверка факта ознакомления сотрудников проверяемого структурного подразделения Института с нормативными документами, регламентирующими вопросы обработки и защиты персональных данных;
- получение при содействии сотрудников проверяемого структурного подразделения Института документов, касающихся обработки и защиты персональных данных в данном структурном подразделении; анализ полученной документации;
- непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

4.5. В ходе осуществления контроля выполнения требований по защите персональных данных в структурном подразделении Института рассматриваются следующие показатели работ по защите персональных данных:

- наличие согласий на обработку персональных данных субъектов персональных данных, в случаях, предусмотренных законодательствам Российской Федерации;
- соответствие состава и сроков обработки целям обработки персональных данных;
- соответствие Перечня должностей Института, замещение которых предусматривает осуществление обработки персональных данных, либо

осуществление доступа к персональным данным фактическому наличию сотрудников;

- соответствие Перечня лиц, имеющих доступ в помещения, в которых ведется обработка персональных данных, фактическому наличию сотрудников;
- наличие нормативных документов по защите персональных данных;
- знание нормативных документов и уровень подготовки сотрудников, имеющих доступ к персональным данным;
- полнота и правильность выполнения требований нормативных документов сотрудниками, имеющими доступ к персональным данным;
- наличие документов, подтверждающих учет и сохранность материальных носителей персональных данных.

4.6. В ходе осуществления контроля выполнения требований по защите персональных данных в структурном подразделении Института дополнительно рассматриваются следующие показатели работ по защите персональных данных:

- соответствие информации, указанной в уведомлении об обработке персональных данных, фактическому состоянию;
- наличие и корректность перечня информационных систем;
- наличие документа, подтверждающего правильность определения
- уровня защищенности персональных данных, обрабатываемых в информационных системах, а также классов защищенности информационных систем;
- наличие документа, подтверждающего факт определения угроз безопасности персональных данных, а также его актуальность (срок актуальности документа не может превышать 3 года);
- соответствие состава средств вычислительной техники информационных систем указанному в документации на информационную систему;
- соответствие требованиям по организации разграничения доступа пользователей к информационным ресурсам (в том числе сетевым);
- порядок защиты персональных данных при передаче по сети;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных.

4.7. Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

4.8. Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

5. Оформление результатов проверки

5.1 Результаты проверки оформляются актом.

5.2 Акт составляется в одном экземпляре и подписывается членами комиссии и хранится у ответственного за организацию обработки персональных данных в Институте. Копия акта передается в проверяемое структурное подразделение Института.

5.3 Результаты проверок подразделений обобщаются ответственным за организацию обработки персональных данных в Института и доводятся до сведения ректора Института.

5.4 При необходимости принятия решений по результатам проверки структурного подразделения Института - ответственным за организацию обработки персональных данных Института готовится соответствующая служебная записка на имя ректора Института.

6. Корректирующие мероприятия и контроль за их исполнением

6.1 Руководитель структурного подразделения Института анализирует акт о результатах внутренней проверки и в пятидневный срок определяет перечень мероприятий, необходимых для устранения нарушений и их причин.

6.2 Перечень мероприятий согласуется с ответственным за организацию обработки персональных данных Института.

6.3 Если корректирующие мероприятия касаются других структурных подразделений Института, то к анализу привлекаются специалисты соответствующих структурных подразделений.

6.4 Выполнение корректирующих мероприятий и их достаточность определяется ответственным за организацию обработки персональных данных Института.

Внутренняя проверка считается оконченной после выполнения всех корректирующих мероприятий и устранения выявленных нарушений.

Приложение 1
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ДОНЕЦКИЙ РЕСПУБЛИКАНСКИЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ»

План
проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных
ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ДОНЕЦКИЙ РЕСПУБЛИКАНСКИЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ»

№	Наименование мероприятия	Период проведения проверки	Отметка о выполнении (№ акта проверки)	Отметка о выполнении корректирующих мероприятий	Примечание