УТВЕРЖДАЮ

Директор

ГБПОУ «НОУОР имени В.С.Тишина»

_____ Е.В. Тряпичников

«14» февраля 2017г.

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям по защите персональных данных

1. Определения и сокращения

Училище - государственное бюджетное профессиональное образовательное учреждение «Нижегородское областное училище олимпийского резерва имени В.С. Тишина» – **оператор персональных данных.**

ПДн - персональные данные, - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

ИСПДн – информационная система персональных данных, представляет собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

Пользователь ИСПДн - работник Училища, осуществляющий на законном основании обработку ПДн в ИСПДн Училища.

Администратор ИСПДн – назначенное директором Училища должностное лицо, уполномоченное на проведение работ по поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах эксплуатации и модернизации, отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты при обработке персональных данных, а также за выявление инцидентов в ИСПДн и реагирование на них.

Правила – утвержденные директором Училища правила осуществления внутреннего контроля соответствия обработки персональных данных в ГБПОУ «НОУОР имени В.С. ТИШИНА» требованиям к защите персональных данных.

АРМ — автоматизированное рабочее место - индивидуальный комплекс технических и программных средств, предназначенный для автоматизации работы Училища;

Субъект персональных данных - это физическое лицо.

2. Общие положения

2.1. Настоящие правила разработаны в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора.

2.2. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Училище и действуют постоянно.

2.3. Целью осуществления внутреннего контроля соответствия обработки персональных данных в Училище, требованиям к защите персональных данных (далее - внутренний контроль) является соблюдение в Училище законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных.

2.4. Внутренний контроль включает в себя: контроль организации защиты информации и контроль эффективности защиты информации.

3. Виды и периодичность внутреннего контроля

1. Внутренний контроль соответствия обработки персональных данных делится на текущий и комиссионный.

2. Текущий внутренний контроль осуществляется на постоянной основе ответственным за обработку персональных данных в ходе мероприятий по обработке персональных данных.

3. Комиссионный внутренний контроль осуществляется комиссией для осуществления внутреннего контроля, он носит периодический характер. Периодичность проверки – не реже одного раза в год.

4. Порядок осуществления внутреннего контроля

3.1. В число основных объектов внутреннего контроля входят:
- структурные и обособленные подразделения Училища, в которых осуществляется обработка ПДн;
- работники, допущенные в установленном порядке к обработке ПДн, и их носителям, и выполняющие работы с их использованием;
- служебные помещения, в которых проводятся работы с носителями ПДн;
- места непосредственного хранения носителей ПДн (хранилища, сейфы, шкафы);
- непосредственно носители ПДн (документы, материалы, изделия, магнитные носители);
- компоненты ИСПДн, в которых осуществляется обработка ПДн;
- локальная сеть передачи данных.

Особенности контроля безопасности ПДн в отдельных ИСПДн могут регулироваться дополнительными локальными актами.

3.2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Училище организовывается проведение периодических проверок условий обработки персональных данных.

3.3. Проверки осуществляются ответственным за организацию обработки персональных данных в Училище либо комиссией, образуемой приказом руководителя Училища.

В проведении проверки не может участвовать работник, прямо или косвенно заинтересованный в её результатах.

3.4. Проверки соответствия обработки персональных данных установленным требованиям в Училище проводятся на основании утвержденного ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в Училище письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

3.5. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- соблюдение принципов обработки ПДн в структурных подразделениях Училища;
- соответствие локальных актов в области ПДн Училища, действующему законодательству;
- выполнение работниками структурных подразделений Училища требований и правил (в том числе особых) обработки ПДн в ИСПДн;
- соответствие перечней ПДн, используемых для решения задач и функций структурными подразделениями Училища и необходимость обработки ПДн в ИСПДн;
- правильность осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи

(распространения, предоставления доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой информационной системе ПДн;

- актуальность перечня должностей работников Училища, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн;
- актуальность перечня должностных лиц, уполномоченных на обработку ПДн, имеющих доступ к ПДн;
- актуальность перечня должностей работников Училища, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;
- актуальность сведений, содержащихся в уведомлении об обработке ПДн;
- актуальность перечня ИСПДн и обрабатываемых ПДн Училища;
- соблюдение прав субъектов ПДн, чьи ПДн обрабатываются в ИСПДн;
- соблюдение обязанностей оператора ПДн, предусмотренных действующим законодательством в области ПДн;
- порядок взаимодействия с субъектами персональных данных, чьи ПДн обрабатываются в ИСПДн, в том числе соблюдение сроков, предусмотренных законодательством в области ПДн, соблюдения требований по уведомлениям, порядка разъяснения субъектам ПДн необходимой информации, порядка реагирования на обращения субъектов ПДн, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами пДн;
- наличие необходимых согласий субъектов ПДн, чьи ПДн обрабатываются в ИСПДн;
- наличие и актуальность сведений, содержащихся в каждой ИСПДн Училища;
- знание и соблюдение работниками Училища положений действующего законодательства Российской Федерации в области ПДн и других локальных актов Училища;
- знание и соблюдение работниками Училища инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение и средства защиты информации;
- соблюдение работниками Училища конфиденциальности ПДн;
- соблюдение работниками Училища требований по обеспечению безопасности ПДн;
- наличие и актуальность локальных актов Училища, технической и эксплуатационной документации технических и программных средств ИСПДн;
- 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 до ввода в эксплуатацию информационной системы 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 восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.
- иных запросов.
- соблюдение пользователями ИСПДн инструкции по организации парольной политики;
- соблюдение пользователями ИСПДн инструкции по организации антивирусной политики;
- соблюдение порядка доступа в помещения Училища, где расположены элементы ИСПДн и где обрабатываются и хранятся бумажные носители с персональными данными.

3.6. Ответственный за организацию обработки персональных данных в Училище (комиссия) имеет право:

- запрашивать у сотрудников организации информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных должностных 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 руководителю Училища предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить руководителю Училища предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

3.7. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в Училище (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

3.8. Срок проведения проверки не может составлять более 30 (тридцати) дней со дня принятия решения о ее проведении. Результаты проверки оформляются в виде письменного заключения, утверждаются председателем комиссии и докладываются директору Училища.