Муниципальное бюджетное образовательное учреждение
дополнительного образования
«Усть-Ишимский Дом детского творчества»

ПРИКАЗ

14.03.2022 г Усть-Ишим № 27

Об утверждении регламента проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Во исполнение требований Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных» и прочих нормативных документов по защите информации, ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Регламент проведения внутреннего контроля соответствия обработки персональных данных в БУ ОО ДО «ЦДНВ «Исток» требованиям к защите персональных данных (далее - Регламент) (Приложение № 1).
2. Требования Регламента довести до работников, непосредственно осуществляющих защиту персональных данных.
3. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор: Зарипова З.А. Зарипова

Приложение № 1
к приказу
МБОУ ДО «Усть-Ишимский ДДТ»
от 14.03.22022 г № 27

РЕГЛАМЕНТ
проведения внутреннего контроля соответствия обработкперсональных данных вМБОУ ДО «Усть-Ишимский ДДТ» требованиям к защите персональных данных

1.1. Регламент проведения внутреннего контроля соответствия обработки персональных данных в МБОУ ДО «Усть-Ишимский ДДТ» требованиям к защите персональных данных (далее - регламент), разработан в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных»; постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; приказом ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; на основании Устава и локальных нормативных актов МБОУ ДО «Усть-Ишимский ДДТ (далее - ДДТ).

1.2. В целях реализации настоящего регламента используются следующие термины и их определения:

1.2.1. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.2.2. Инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.2.3. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

1.2.5. Средство защиты информации - программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

1.3. Настоящий регламент утверждается приказом директора.

1.4. Изменения и дополнения в настоящий регламент утверждаются приказом директора.

1.5. Настоящий регламент является локальным нормативным актом, регламентирующим деятельность ДДТ.

1.6. Срок действия настоящего регламента не ограничен и действует до принятия нового регламента.

1.7. Настоящий регламент подлежит пересмотру не реже одного раза в три года.

2. Общие положения

2.1. Настоящий регламент определяет порядок проведения внутреннего контроля соответствия обработки персональных данных (далее - Внутренний контроль), требованиям к защите персональных данных.

2.2. Регламент обязателен для исполнения ответственным за организацию обработки персональных данных, ответственным за обеспечение безопасности и администратором информационных систем персональных данных.

3. Порядок проведения внутреннего контроля

3.1. Для проведения внутреннего контроля в информационных системах приказом директора ДДТ создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:

– ответственного за обеспечение безопасности персональных данных в информационных системах;

– ответственного за организацию обработки персональных данных.

3.2. В случае временного отсутствия (болезнь, отпуск, пр.) ответственных, в состав комиссии включаются лица их замещающие.

3.3. Допускается привлечение к проверкам сторонних экспертных организаций.

3.4. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками ДДТ, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам внутреннего контроля, которое передается на рассмотрение директору ДДТ.

3.5. Внутренний контроль проводится в соответствии с «Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных», утвержденным приказом директора ДДТ, форма которого приведена в ***Приложении 1*** к настоящему Регламенту.

3.6. В «Плане проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» указывается перечень проводимых мероприятий внутреннего контроля и периодичность их проведения.

3.7. Комиссия проводит внутренний контроль непосредственно на месте обработки персональных данных, опрашивает работников ДДТ, осуществляющих обработку персональных данных, осматривает рабочие места.

3.8. При проведении внутреннего контроля должен присутствовать руководитель проверяемого подразделения.

3.9. В ходе проведения внутреннего контроля осуществляется:

– контроль выполнения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах, необходимых для выполнения требований к защите персональных данных;

– анализ изменения угроз безопасности персональных данных в информационных системах, возникающих в ходе их эксплуатации;

– проверка параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (далее - СЗИ);

– контроль состава технических средств, программного обеспечения и СЗИ;
– состояние учета СЗИ;
– состояние учета средств шифровальной (криптографической) защиты информации;
– состояние учета съемных машинных носителей персональных данных;
– соблюдение правил доступа к персональным данным;
– контроль наличия (отсутствия) фактов несанкционированного доступа к персональным данным;
– соблюдение пользователями парольной политики;
– соблюдение пользователями антивирусной политики;
– соблюдение пользователями правил работы со съемными машинными носителями;
– контроль соблюдения работниками требований локальных нормативных актов, в т.н. требований законодательства по вопросам обработки и защиты персональных данных;
– выявление уязвимостей в информационных системах с использованием специализированных средств инструментального анализа защищенности.

3.10. Все работники обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения по существу заданных им вопросов.

3.11. По завершении внутреннего контроля комиссией составляется «Акт о проведении контроля соответствия обработки персональных данных», форма которого приведена в Приложении 2 к настоящему регламенту.

3.12. В «Акте о проведении контроля соответствия обработки персональных данных» указываются:

– перечень проведенных мероприятий;
– выявленные нарушения;
– мероприятия по устранению нарушений;
– решения по результатам внутреннего контроля;
– сроки устранения нарушений.

3.13. Периодичность проведения внутреннего контроля составляет не реже 1 раза в год.

3.14. Предложения о создании комиссии и о плановом/внеплановом проведении внутреннего контроля представляются директору ДДТ ответственным за организацию обработки персональных данных и ответственным за обеспечение безопасности персональных данных в информационных системах.

3.15. Внеплановый контроль проводится в следующих случаях:

– наличие подозрений на нарушение требований по защите персональных данных;
– наличие подозрений на осуществление попыток несанкционированного доступа к персональным данным;
– наличие подозрений на сбой в работе технических средств информационных систем персональных данных, в т.ч. средств защиты информации;
– предстоящая проверка надзорными органами.

3.16. Порядок проведения внепланового контроля совпадает с порядком проведения планового контроля.

3.17. При выявлении в ходе планового/внепланового контроля нарушений требований по обработке и защите персональных данных осуществляется оперативное устранение выявленных нарушений.

3.18. Выявленные нарушения должны быть устранены в срок не превышающий 30 дней с момента утверждения «Акта о проведении контроля соответствия обработки персональных данных».

3.19. По истечению срока, данного на устранение замечаний, комиссия проводит

повторный контроль.

4. Ответственность

4.1. Ответственный за организацию обработки персональных данных в ДДТ несет ответственность за организацию проведения внутреннего контроля соответствия обработки персональных данных в ДДТ требованиям к защите персональных данных.

Приложение 1
к Регламенту проведения внутреннего контроля соответствия обработки персональных данных в МБОУ ДО «Усть-Ишимский ДДТ» требованиям к защите персональных данных

ФОРМА

План проведения внутреннего контроля соответствия обработки персональных данных в МБОУ ДО «Усть-Ишимский ДДТ»

№ п/п	Мероприятие	Регулярность проведения
1.	Анализ актуальности локальных нормативных актов (внутренних документов) по вопросам обеспечения безопасности персональных данных: - Проверка соответствия локальных нормативных актов (внутренних документов) по вопросам обеспечения безопасности персональных данных действующему законодательству РФ по защите персональных данных; - Учет в локальных нормативных актах (внутренних документах) по вопросам обеспечения безопасности персональных данных изменений в деятельности МБОУ ДО «Усть-Ишимский ДДТ»по обработке и защите персональных данных.	1 раз в три года или по мере обновления законодательства РФ
2.	Проверка ознакомления работников с положениями законодательства РФ по защите персональных данных, документами, определяющими политикуМБОУ ДО «Усть-Ишимский ДДТ» в отношении обработки персональных данных и организационно-распорядительными документами по вопросам персональных данных.	1 раз в год
3.	Проверка выполнения работниками - пользователями информационных систем персональных данных инструкций по эксплуатации информационных систем персональных данных, положения о разрешительной системе доступа.	1 раз в год
4.	Проверка актуальности прав разграничения доступа пользователей информационных систем персональных данных, необходимых для выполнения должностных обязанностей.	1 раз в год
5.	Проверка актуальности определенных угроз безопасности персональных данных для информационных систем персональных данных.	1 раз в год
6.	Проверка полноты реализованных технических мер по обеспечению безопасности персональных данных в информационных системах персональных данных с учетом структурно-функциональных характеристик информационных системах персональных данных, информационных технологий, особенностей функционирования информационных системах персональных данных.	1 раз в год
7.	Проверка наличия сертифицированных средств защиты информации, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных	1 раз в год
8.	Проверка правил обращения со съемными машинными носителями персональных данных.	1 раз в год

9.	Проверка актуальности информации, содержащейся в Уведомлении об обработке персональных данных, предоставленной в Роскомнадзор.	1 раз в год
10.	Проверка соответствия условий использования средств криптографической защиты условиям, предусмотренным эксплуатационной и технической документацией к ним.	1 раз в год
11.	Выявление уязвимостей в информационных системах персональных данных в т.ч. в системе защиты с использованием средства инструментального анализа защищенности.	1 раз в год

Приложение 2
к Регламенту проведения внутреннего контроля соответствия обработки персональных данных в МБОУ ДО «Усть-Ишимский ДДТ» требованиям к защите персональных данных

ФОРМА

04.03.2022 г Усть-Ишим № 16

АКТ
О проведении контроля соответствия обработки персональных данных

Комиссия в составе:
Председатель: _____ _____
Члены комиссии:
1 _____ _____
2 _____ _____
3 _____ _____

составила настоящий акт о том, что комиссией были проведены мероприятия по контролю соответствия обработки персональных данных в МБУ ДО «Усть-Ишимский ДДТ» требованиям к защите персональных данных. Результат проведенного внутреннего контроля отражен в Таблице 1.

Таблица 1

№ п/п	Мероприятие	Выявленные недостатки	Мероприятия по устранению недостатков	Срок проведения мероприятий	Ответственное лицо

Внутренний контроль проводился в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в МБОУ ДО «Усть-Ишимский ДДТ» требованиям к защите персональных данных».

Председатель: _____ _____
Члены комиссии:
4 _____ _____
5 _____ _____
6 _____ _____