Муниципальное бюджетное учреждение дополнительного образования
«Центр детского и юношеского творчества»
муниципального образования городской округ Симферополь
Республики Крым

УТВЕРЖДАЮ
Директор МБ УДО «ЦДЮТ»
г. Симферополя
_____ Т.С. Ельцова
Приказ №10 от 10.01.2022 г.

РЕГЛАМЕНТ
ПРОВЕДЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В МБ УДО «ЦДЮТ» ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Термины и определения

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

1.2. 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 Положения или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.3. 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.

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

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

2. Общие положения

2.1. Настоящий Регламент проведения внутреннего контроля соответствия обработки персональных данных в МБ УДО «ЦДЮТ» требованиям к защите персональных данных (далее – Регламент), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящий Регламент определяет порядок проведения внутреннего контроля соответствия обработки ПДн (далее – Внутренний контроль), требованиям к защите ПДн.

2.3. Регламент обязателен для исполнения ответственным за организацию обработки ПДн, ответственным за обеспечение безопасности ПДн.

3. Порядок проведения внутреннего контроля

3.1. Для проведения внутреннего контроля в ИСПДн приказом директора создаётся комиссия, состоящая из трех человек с обязательным включением в её состав:

- Ответственного за обеспечение безопасности ПДн в ИСПДн;
- ответственного за организацию обработки ПДн.

3.2. Допускается привлечение к проверкам сторонних экспертных организаций.

3.3. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с работниками Центра, готовит и ведёт заседания комиссии, готовит заключение по результатам внутреннего контроля, которое передается на рассмотрение директору.

3.4. Внутренний контроль проводится в соответствии с «Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных», утвержденным приказом директора.

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

3.6. Комиссия проводит внутренний контроль непосредственно на месте обработки ПДн, опрашивает работников Центра, осуществляющих обработку ПДн, осматривает рабочие места.

3.7. В ходе проведения внутреннего контроля осуществляется:

–контроль выполнения организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн;

– анализ изменения угроз безопасности ПДн в ИСПДн, возникающих в ходе ее 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 ПДн;

– соблюдение правил доступа к ПДн;

– контроль наличия (отсутствия) фактов несанкционированного доступа к ПДн;

–соблюдение пользователями ИСПДн правил работы со съемными машинными носителями ПДн;

– контроль соблюдения работниками требований локальных нормативных актов, в т.ч. требований законодательства по вопросам обработки и защиты ПДн;

– выявление уязвимостей в ИСПДн с использованием специализированных средств инструментального анализа защищенности.

3.8. 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.

3.9. По завершении внутреннего контроля комиссией составляется «Акт о проведении контроля соответствия обработки персональных данных» (Приложение 2).

3.10. 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.

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

3.12. Предложения о создании комиссии и о плановом/внеплановом проведении внутреннего контроля представляются директору ответственным за организацию обработки ПДн и ответственным за обеспечение безопасности ПДн в ИСПДн.

3.13. Внеплановый контроль проводится в следующих случаях:

- наличие подозрений на нарушение требований по защите ПДн;

– наличие подозрений на осуществление попыток несанкционированного доступа к ПДн;

– наличие подозрений на сбой в работе технических средств ИСПДн, в т.ч. средств защиты информации;

– предстоящая проверка надзорными органами.

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

3.15. При выявлении в ходе планового/внепланового контроля нарушений требований по обработке и защите ПДн осуществляется оперативное устранение выявленных нарушений.

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

3.17. По истечению срока, данного на устранение замечаний, комиссия проводит повторный контроль.

4. Ответственность

4.1. Ответственный за организацию обработки ПДн в Центре несет ответственность за организацию проведения внутреннего контроля соответствия обработки ПДн в учреждении требованиям к защите ПДн.

5. Срок действия и порядок внесения изменений

5.1. Настоящий Регламент вступает в силу с момента его утверждения и действует бессрочно, до замены новым Регламентом.

5.2. Изменения и дополнения в настоящий Регламент вносятся приказом директора.

Приложение 1 к Регламенту

ФОРМА

План проведения внутреннего контроля соответствия обработки персональных данных в МБ УДО «ЦДЮТ»

№ 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 МБ УДО «ЦДЮТ» 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 политику МБ УДО «ЦДЮТ» 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 данных.	1 раз в год
8.	Проверка правил обращения со съемными машинными носителями персональных данных.	1 раз в год
9.	Проверка соответствия условий использования средств криптографической защиты условиям, предусмотренным эксплуатационной и технической документацией к ним.	1 раз в год
10.	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

ФОРМА

АКТ

«___» _____ 20__ г. № _____

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 МБ УДО «ЦДЮТ» 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 МБ УДО «ЦДЮТ» требованиям к защите персональных данных».

Председатель:

_____ _____ _____

Члены комиссии:

_____ _____ _____

_____ _____ _____

_____ _____ _____