Приложение № 6 к приказу
Муниципального бюджетного учреждения
дополнительного образования
«Детская школа искусств»
города Вышний Волочек Тверской области от
01 декабря 2021 г. № 38-ОД

Инструкция
по работе администратора безопасности информации в информационной системе персональных данных Муниципального бюджетного учреждения дополнительного образования «Детская школа искусств» города Вышний Волочек

1. **Общие положения.**

а) Администратор безопасности информации (далее – АБИ) в информационной системе персональных данных (далее – ИСПДн) назначается из числа сотрудников Муниципального бюджетного учреждения дополнительного образования «Детская школа искусств» города Вышний Волочек (далее – Учреждение) приказом директора и отвечает за обеспечение требуемого уровня защищенности персональных данных при их обработке в ИСПДн.

б) Администратор безопасности информации в своей работе руководствуется требованиями руководящих документов по обеспечению безопасности персональных данных, положениями нормативно-правовых актов РФ, приказами, а также положениями настоящей Инструкции.

в) Администратор безопасности информации является лицом, обеспечивающим безопасность персональных данных, обрабатываемых, передаваемых и хранимых в ИСПДн.

г) Методическое руководство работой АБИ осуществляется ответственным за организацию обработки персональных данных в ИСПДн.

2. **Обязанности администратора безопасности информации ИСПДн.**

Администратор безопасности информации обязан:

а) четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по обеспечению безопасности персональных данных при их обработке в ИСПДн и распоряжений, регламентирующих порядок действий по обеспечению безопасности персональных данных;

б) управлять средствами защиты информации (далее - СЗИ) ИСПДн и поддержание их функционирования;

в) восстанавливать функции программных и технических СЗИ от несанкционированного доступа (далее - НСД) к информации;

г) обеспечивать функционирование ИСПДн в пределах возложенных функций;

д) генерировать ключи, личные идентификаторы, а также пароли для пользователей ИСПДн;

е) формировать и управлять списком необходимых реквизитов и значением атрибутов объектов и субъектов доступа;

ж) назначать права доступа, полномочия и привилегии пользователей к объектам доступа (программам, файлам, каталогам, портам и устройствам ввода-вывода);

з) обеспечивать правильную эксплуатацию технических и программных СЗИ в ИСПДн;

и) контролировать целостность эксплуатируемого в ИСПДн программного обеспечения, в том числе самих СЗИ, с целью недопущения и выявления несанкционированных модификаций;

к) выявлять, анализировать и устранять уязвимости и иные недостатки в программном обеспечении;

л) в случае нарушения работоспособности (отказе) технических средств и программного обеспечения ИСПДн, в том числе СЗИ, немедленно докладывать о случившемся ответственному за обеспечение безопасности персональных данных в ИСПДн;

м) осуществлять текущий, после сбоев и периодический (не реже 1 раза в год) контроль работоспособности средств и систем защиты информации;

н) выполнять и контролировать выполнения установленного комплекса мероприятий по обеспечению безопасности персональных данных при их обработке в ИСПДн;

о) проводить инструктаж и консультации пользователей ИСПДн по соблюдению установленного режима конфиденциальности при обработке персональных данных в ИСПДн;

п) контролировать соблюдение пользователями ИСПДн требований инструкций и порядка работы при обработке информации в ИСПДн по вопросам защиты информации от НСД;

р) взаимодействовать с ответственным за организацию обработки персональных данных в Учреждении и ответственным за обеспечение безопасности персональных данных в ИСПДн по вопросам обеспечения безопасности персональных данных при их обработке в ИСПДн и соблюдении прав доступа пользователей к ней;

с) выполнять и учитывать изменения, вносимые:

– в списки пользователей ИСПДн;

– в перечень защищаемых информационных ресурсов ИСПДн;

т) контролировать выполнение утвержденной технологии обработки персональных данных в ИСПДн;

у) контролировать состав технических средств, программного обеспечения и средств зашиты информации;

ф) контролировать установку и обновление программного обеспечения, запрет установки неразрешённого программного обеспечения (в том числе средств обработки и отладки);

х) выявлять подозрительные действия пользователей и попытки НСД к информации, обрабатываемой в ИСПДн, путем анализа системных журналов информационной безопасности при работе в ИСПДн;

ц) выполнять резервное копирование машинных документов, содержащих персональные данные;

ч) обучать и консультировать пользователей ИСПДн правилам работы с СЗИ от НСД;

ш) проводить антивирусную защиту информации и программных средств в ИСПДн;

щ) контролировать электронный журнал сообщений и обеспечивать доступ к нему лиц, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;

ы) просматривать и анализировать результаты регистрации событий, относящихся к безопасности персональных данных, и реагировать на них;

э) контролировать безотказное функционирование технических и программных средств, принимать меры по восстановлению отказавших средств;

ю) обеспечивать строгое выполнение требований по обеспечению безопасности персональных данных при организации обслуживания технических средств ИСПДн и отправке их в ремонт;

я) обеспечивать соответствие состава ИСПДн техническому паспорту на ИСПДн (в т.ч. реальной конфигурации информационных связей).

3. Права администратора безопасности информации ИСПДн.

Администратор безопасности информации имеет право:

а) требовать от пользователей ИСПДн выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных;

б) участвовать в разработке мероприятий Учреждения по совершенствованию безопасности персональных данных;

в) останавливать обработку информации в ИСПДн в случаях подтвержденных нарушений установленной технологии обработки персональных данных, приводящих к нарушению функционирования СЗИ;

г) подавать свои предложения по совершенствованию технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн.