Приложение № 1
к приказу
от «21» 12. 2017 г. № 56

Инструкция
администратора безопасности ИСПДн МБОУ ДО «Гавриловская школа искусств»

1. Общие положения

1.1 Администратор безопасности информационных систем персональных данных МБОУ ДО «Гавриловская школа искусств» (далее – Администратор) отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) в процессе их обработки в информационных системах персональных данных (далее – ИСПДн) Учреждения.

1.2 Администратор должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн.

1.3 В своей деятельности Администратор руководствуется Положением об обработке и защите персональных данных в МБОУ ДО «Гавриловская школа искусств» и настоящей Инструкцией, рекомендациями ответственного за организацию обработки персональных данных (далее – ответственный за организацию обработки ПДн), ответственного за обеспечение безопасности персональных данных.

2. Основные функции и обязанности Администратора безопасности персональных данных в информационных системах персональных данных

2.1 Администратор изучает все стороны деятельности Учреждения и вырабатывает рекомендации по защите ПДн при решении следующих основных вопросов:

– проведение аналитической работы по комплексной защите и предупреждению утечки ПДн;

– подготовка решений в отношении сведений о работах, выполняемых Учреждением, подлежащих защите;

– рассмотрение проектов технических заданий, нормативных актов и указаний, договоров на выполнение работ, отчетной документации, с целью определения достаточности предусмотренных в них требований и мероприятий по комплексной защите ПДн, при научных исследованиях, при проведении других работ;

– координация внедрения и эксплуатации систем защиты и безопасности информации, обрабатываемой техническими средствами;

– проведение работ по контролю эффективности принимаемых мер по выявлению и закрытию возможных каналов утечки ПДн;

– подготовка предложений по совершенствованию действующей системы защиты ПДн;

– учет, администрирование применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;

– обеспечение соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;

– осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Учреждения.

Администратор обязан:

2.2 Соблюдать требования действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн.

2.3 Знать состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку ПДн.

2.4 Осуществлять общее техническое сопровождение ИСПДн:

– контролировать соблюдение требований по размещению и использованию технических средств, указанных в инструкциях по эксплуатации этих средств;

– контролировать сохранность пломб на оборудовании автоматизированных рабочих мест;

– вести журнал учета и выдачи используемых материальных носителей ПДн;

– контролировать использование съемных материальных носителей информации, в том числе запрещать использование неучтенных носителей информации;

– проводить инструктаж сотрудников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в ИСПДн Учреждения (далее – Пользователи ИСПДн) по правилам работы в ИСПДн.

2.5 Осуществлять настройку и сопровождение подсистемы регистрации и учета ИСПДн:

– реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководителем списка сотрудников, допущенных к работе в ИСПДн;

– управлять (присваивать, уничтожать) идентификаторы (имена пользователя) и аутентификаторы (пароли, аппаратные идентификаторы) пользователей ИСПДн ИСПДн;

– контролировать плановую смену паролей Пользователями ИСПДн для доступа в ИСПДн;

– управлять (заведение, активация, блокирование, уничтожение) учётными записями пользователей ИСПДн;

– своевременно удалять профиль Пользователя ИСПДн при увольнении или переводе сотрудника;

– вводить в базу данных системы защиты от несанкционированного доступа (далее – НСД) описания событий, подлежащих регистрации в системном журнале;

– регулярно проводить анализ системного журнала для выявления инцидентов безопасности, попыток несанкционированного доступа к ИСПДн;

– своевременно информировать ответственного за обеспечение безопасности ПДн о несанкционированных действиях персонала для организации расследования инцидентов (попыток НСД).

2.6 Сопровождать подсистему обеспечения целостности рабочего программного обеспечения (ПО) ИСПДн:

– обеспечивать регулярное и своевременное обновление антивирусного программного обеспечения Учреждения;

– обеспечивать поддержание установленного порядка эксплуатации антивирусного программного обеспечения;

– обеспечивать регулярное и своевременное создание резервных копий ИСПДн Учреждения;

– осуществлять настройку и сопровождение системы защиты от НСД в ИСПДн.

2.7 Проводить периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий Пользователей ИСПДн.

2.8 Требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

2.9 Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и служебных расследований инцидентов безопасности. Принимать меры по устранению последствий инцидентов и планировать и принанимать меры по предотвращению повторного возникновения инцидентов

2.10 Участвовать при проведении внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн.

2.11 Контролировать выполнение Пользователями ИСПДн требований Инструкций а также установленных требований для обеспечения уровней защищенности ПДн.

2.12 Контролировать правильность применения Пользователями ИСПДн средств защиты информации.

2.13В случае получения от Пользователей ИСПДн информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, незамедлительно принять все необходимые меры для обеспечения безопасности ПДн в пределах своих полномочий.

2.14 Обеспечивать функционирование и поддерживать работоспособность на автоматизированных рабочих местах ИСПДн:

- антивирусного программного обеспечения;
- средств защиты от несанкционированного доступа.

2.15 В случае нарушения работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.

2.16 Своевременно информировать ответственного за обеспечение безопасности ПДн (или руководителя Учреждения) о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа к ИСПДн.

2.17 Выполнять действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных.

3. Права Администратора безопасности персональных данных в информационных системах персональных данных

Администратор имеет право:

3.1 Знакомиться с нормативными актами Учреждения, регламентирующими процессы обработки и защиты ПДн.

3.2 Вносить предложения руководителю Учреждения по совершенствованию существующей системы защиты информации.

3.3 Привлекать по согласованию Администратором за организацию обработки ПДн и руководителем Учреждения к работе по созданию и совершенствованию системы защиты ПДн других сотрудников Учреждения.

3.4 Требовать от Пользователей ИСПДн соблюдения требований Инструкций а также соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн.

3.5 Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность ПДн, вносить свои предложения по совершенствованию организационных и технических мер защиты ПДн в ИСПДн.

3.6 Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн.

3.7 Требовать прекращения работы в ИСПДн, как в целом, так и отдельных Пользователей ИСПДн, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ИСПДн.

3.8 Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к ответственным лицам Учреждения.