Экз. № 1

УТВЕРЖДАЮ
Директор
МБУ «Школа № 70»
_____ О.Б. Жигулевцева
«31» августа 2018 г.
Приказ № 97/5-ОД

ИНСТРУКЦИЯ
Администратора информационной безопасности

Персональные компьютеры, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование принадлежат МБУ «Школа № 70» (далее - Школа) и предоставляются работникам для осуществления ими своих должностных обязанностей.

АРМ, имеющие подключение к ЛВС и не имеющие подключение к ЛВС, серверы, ПО, оборудование ЛВС, коммуникационное оборудование, пользователи - образуют систему Объекта информатизации (ОИ).

АРМ - автоматизированное рабочее место;
ПО - программное обеспечение;
ЛВС - локально-вычислительная сеть;
ОИ - объект информатизации;
ОВТ - объект вычислительной техники (составная часть ОИ);
НСД - несанкционированный доступ;
СЗИ - система защиты информации.

Конфиденциальная информация, в том числе персональные данные - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации; характер сведений, обуславливающий их сбор, обработку и распространение на условиях соответствующего правового режима. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом № 152-ФЗ «О персональных данных».

1 Общие положения

1.1 Настоящая Инструкция разработана с целью приведения в соответствие с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и исполнения законодательных требований при обработке персональных данных в МБУ «Школа № 70» и является руководством по работе с персональными данными и компьютерами сети Школы. Целью настоящей Инструкции является регулирование работы Администратора информационной безопасности, распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации, более эффективного использования сетевых ресурсов и уменьшения риска умышленного или неумышленного нарушения порядка работы с персональными данными.

1.2 Настоящая Инструкция определяет основные обязанности, права и ответственность Администратора информационной безопасности Школы.

1.3 Администратор информационной безопасности назначается Приказом директора Школы и отвечает за обеспечение устойчивой работоспособности и информационной безопасности объекта информатизации.

1.4 Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности Администратора информационной безопасности.

1.5 Администратор информационной безопасности обладает всеми правами доступа к любым программным и аппаратным ресурсам, любой информации на рабочих станциях пользователей Школы (за исключением информации, закрытой с использованием средств криптозащиты) и средствам их защиты.

1.6 Администратор информационной безопасности несет ответственность за реализацию принятой в Школе политики безопасности, регламентированной Положениями о защите персональных данных работников, обучающихся и родителей (законных представителей) обучающихся, Регламентом использования технических средств и действующими приказами и распоряжениями.

1.7 Администратор информационной безопасности должен ознакомиться с настоящей Инструкцией, под личную подпись.

2 Основные обязанности Администратора информационной безопасности

2.1 При выполнении своих должностных обязанностей Администратор информационной безопасности выполняет следующие функции:

- Осуществляет установку, настройку и сопровождение локальной вычислительной сети Школы.

- Обеспечивает надлежащий уровень безопасности и сохранности данных, соблюдение прав доступа и уменьшение риска умышленного или неумышленного нарушения регламента работы с персональными данными и объекта информатизации в целом.

2.2 Осуществляет подключение вновь вводимых компьютеров к ЛВС на основании служебной записки за подписью ответственных руководителей подразделений Школы.

2.3 Создает, на основании служебных записок за подписью руководителей подразделений новые учетные записи и назначает пароли для первоначального доступа к ОВТ вновь заводимым пользователям Школы.

2.4 Определяет, на основании служебных записок за подписью руководителей подразделений и согласно «Положениям о защите персональных данных...», действующих в Школе, права доступа (чтение, запись, редактирование и т.п.) для каждого пользователя и/или группы пользователей к защищаемым информационным ресурсам (томам, каталогам, файлам, базам данных и т.д.).

2.5 Своевременно отслеживает текущее состояние учетных записей пользователей при кадровых изменениях у владельцев учетных записей.

2.6 Обеспечивает, на основании «Регламента резервного копирования данных...», регулярное создание резервных копий данных с сетевых файловых ресурсов и сетевых баз данных.

2.7 Контролирует интенсивность использования общих сетевых ресурсов, дискового пространства файловых хранилищ и дискового пространства используемых баз данных Школы.

2.8 Обеспечивает регулярное обновление антивирусного программного обеспечения на рабочих станциях Школы.

2.9 Осуществляет на основании «Плана внутренних проверок режима защиты персональных данных в ИСПДн…» мероприятия по проверке режима защиты персональных данных, в том числе функционирование средств защиты информации, которое должно быть отражено в «Журнале функционирования средств защиты информации…».

2.10 Проводит инструктаж работников Школы по вопросам информационной безопасности, который должен быть отражен в «Журнале инструктажа работников МБУ «Школа № 70» по вопросам информационной безопасности».

2.11 Обеспечивает и контролирует доступ работников Школы к внешним WEB ресурсам сети Интернет и электронной почте.

2.12 Осуществляет установку, настройку и модификацию/обновление программного обеспечения для обеспечения доступа и контроля доступа к сети Интернет и электронной почте.

2.13 Обеспечивает фильтрацию вредоносного и нерегламентированного контента, посещаемых WEB ресурсов в сети Интернет и спам содержимого входящей электронной почты Школы.

2.14 Обеспечивает надлежащий уровень безопасности локальной вычислительной сети и сетевых ресурсов Школы от возможных внешних сетевых воздействий посторонних лиц.

2.15 Осуществляет настройку, ведение и регулярный анализ системных журналов для своевременного выявления попыток несанкционированного доступа к защищаемым информационным ресурсам объектов вычислительной техники.

2.16 Своевременно информирует руководство Школы о выявленных фактах несанкционированных действий работников Школы и противоправных действиях третьих лиц.

3 Права Администратора информационной безопасности

3.1 Осуществлять контроль за выполнением пользователями требований Инструкции пользователей по безопасной обработке персональных данных на объектах вычислительной техники.

3.2 Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ОВТ.

3.3 Непосредственно обращаться к руководителям подразделений Школы с требованием прекращения работы на объекте вычислительной техники при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

3.4 Вносить свои предложения по совершенствованию мер защиты объектов вычислительной техники.

4 Ответственность Администратора информационной безопасности

4.1 Администратор информационной безопасности несет ответственность за организацию работ по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи объектов вычислительной техники (ОВТ), а также правильность использования и нормального функционирования средств защиты информации (СЗИ), подготовку и консультацию работников по вопросам безопасной обработки информации на ОВТ.

4.2 Администратор информационной безопасности отвечает за бесперебойное функционирование вверенных ему ресурсов ОИ, качество

предоставляемых пользователям сервисов.

4.3 На Администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации Школы.

Лист ознакомления работников

№ п/п	Ф.И.О.	Дата	Подпись