Экз. № 1

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

ИНСТРУКЦИЯ
Ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных

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;
ОТСС - основные технические средства и системы;
ВТСС - вспомогательные технические средства и системы;
ИСПДн - информационная система персональных данных;
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», Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», и исполнения законодательных требований при обработке персональных данных в Школе и является руководством по работе с персональными данными и компьютерами сети Школы. Целью настоящей Инструкции является регулирование работы Ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных (далее – Ответственный за обеспечение безопасности персональных данных в ИСПДн), поддержания необходимого уровня защиты информации, обрабатываемой в ИСПДн 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 Ответственного за обеспечение безопасности персональных данных в Школе.

2 Основные обязанности Ответственного за обеспечение безопасности персональных данных в ИСПДн

2.1 Для разработки и осуществления мероприятий по организации и обеспечению безопасности персональных данных при их обработке в ИСПДн Школы назначить должностное лицо, ответственное за обеспечение безопасности персональных данных.

2.2 В обязанности Ответственного за обеспечение безопасности персональных данных в ИСПДн входит:

1) Обеспечить безопасность персональных данных, включая установление типа актуальных угроз и определение уровней защищенности персональных данных при их обработке в ИСПДн;
2) Организовать защиту персональных данных от несанкционированного доступа и определение порядка выбора средств защиты персональных данных при их обработке в ИСПДн;
3) Провести инвентаризацию всех неучтенных ОТСС и ВТСС;
4) Осуществить контроль за использованием лицензионного ПО на рабочих станциях Школы;
5) Осуществить контроль за использованием сертифицированного антивирусного ПО на рабочих станциях Школы;

6) Регулярно проводить проверки рабочих станций пользователей сертифицированными антивирусными программами на наличие вредоносного кода;

7) Удалять с рабочих станций пользователей программное обеспечение (ПО), не используемое для выполнения служебных обязанностей;

8) Обновлять операционную систему на рабочих станциях до сертифицированной версии;

9) Установить порядок внесения дополнений и изменений в конфигурацию и монтаж технических систем и средств;

10) Систематически проверять состояние и работоспособность всех средств и механизмов защиты;

11) Обеспечить защиту данных регистрации от их уничтожения или модификации нарушителем;

12) Реализовать механизмы сохранения данных регистрации в случае сокращения отведенных под них ресурсов.

3 Права Ответственного за обеспечение безопасности персональных данных в ИСПДн

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.

3.5 Участвовать в разработке мероприятий по совершенствованию безопасности персональных данных в ИСПДн.

4 Ответственность

4.1 Ответственный за обеспечение безопасности персональных данных в ИСПДн отвечает за безопасность персональных данных в ИСПДн Школы.

4.2 Ответственный за обеспечение безопасности персональных данных в ИСПДн несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

4.3 Ответственный за обеспечение безопасности персональных данных в ИСПДн, виновный в нарушении норм, регулирующих получение, обработку и защиту персональных данных привлекается к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом и иными федеральными законами, а также привлекается к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Лист ознакомления работников

№ п/п	Ф.И.О.	Дата	Подпись