Согласовано
Председатель профкома:
_____ Касаткина О.В.
Протокол № 11 от 29.08.2014г.

Утверждаю
Директор МОУ Иванковской СОШ:
_____ Г.В. Жаренова
Приказ № 175 от 01.09.2014г

ИНСТРУКЦИЯ АДМИНИСРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор безопасности информационной системы персональных данных (ИСПДн) (далее – Администратор безопасности ИСПДн) назначается приказом директора МОУ Иванковской СОШ, на основании Положения о разграничении прав доступа к обрабатываемым персональным данным.

1.2. Администратор безопасности ИСПДн подчиняется, лицу назначенному ответственным за организацию обработки персональных данных в МОУ Иванковской СОШ (далее – Учреждение).

1.3. Администратор безопасности ИСПДн в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Учреждения.

1.4. Администратор безопасности ИСПДн отвечает за поддержание необходимого уровня безопасности объектов защиты.

1.5. Администратор безопасности ИСПДн является ответственным должностным лицом в Учреждении, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты информационной системы персональных данных (далее – ИСПДн) и ее ресурсов на этапах промышленной эксплуатации, модернизации и выводе из эксплуатации.

1.6. Администратор безопасности ИСПДн должен иметь специальное рабочее место, размещенное в здании Учреждения так, что бы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. Рабочее место Администратора безопасности ИСПДн должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое).

1.8. Администратор безопасности ИСПДн осуществляет методическое руководство пользователями информационной системы и Администратором ИСПДн, в вопросах обеспечения безопасности персональных данных.

1.9. Требования Администратора безопасности ИСПДн, связанные с выполнением им своих должностных (возложенных) обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.10. Администратор безопасности ИСПДн несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Администратор безопасности ИСПДн обязан:

- знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации;
- осуществлять установку, настройку и сопровождение технических средств защиты;
- участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн;
- участвовать в приеме новых программных средств;

– обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения;

– уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты;

– вести контроль над процессом осуществления резервного копирования объектов защиты;

– осуществлять контроль над выполнением Плана мероприятий по защите персональных данных;

– анализировать состояние защиты ИСПДн и ее отдельных подсистем;

– контролировать неизменность состояния средств защиты их параметров и режимов защиты;

– контролировать физическую сохранность средств и оборудования ИСПДн;

– контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты;

– контролировать исполнение пользователями парольной политики;

– контролировать работу пользователей в сетях общего пользования и (или) международного обмена;

– своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;

– не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач;

– не допускать к работе на элементах ИСПДн посторонних лиц;

– осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн;

– оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты;

– периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации;

– в случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

– принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

–

3. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором безопасности ИСПДн или Администратором ИСПДн.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

– пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

– пароль должен состоять не менее чем из 8 символов.

– в пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

– запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

– запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

– запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– запрещается выбирать пароли, которые уже использовались ранее.

4. ПРАВА И ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Администратор безопасности ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с его полномочиями в отношениях к ресурсам ИСПДн и вверенным ему техническим и программным средствам. В частности, Администратор безопасности ИСПДн имеет право:

- проверять электронный журнал обращений
- вносить изменения в конфигурацию аппаратно-программных средств
- проверять соблюдение условий использования средств защиты информации
- требовать прекращения обработки информации как в целом, так и отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования автоматизированного рабочего места (АРМ).

3.2 Администратор безопасности ИСПДн, виновный в несоблюдении Настоящей инструкции расценивается как нарушитель Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и несет предусмотренную законодательством Российской Федерации ответственность.

С инструкцией ознакомлен,
один экземпляр получил: _____ _____
(подпись) (фамилия, инициалы)

Принято на заседании общего собрания
работников МОУ Иванковской СОШ
Протокол №____ от _____ 2014г