УТВЕРЖДАЮ
Директор МБОУ «СОШ №31» НМР РТ
_____И.А. Габдуллахатов
Приказ №97
от «12» марта 2018 г.

Инструкцию для администраторов безопасности конфиденциальной информации, в том числе ПДн, информационных систем персональных данных, резервирования и восстановления работоспособности ПО, баз данных и СЗПДн

1. Общие положения

1.1. Администратор ИСПДн (далее – Администратор) назначается приказом руководителя.

1.2. Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами ОУ.

1.3. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

2. Должностные обязанности

Администратор обязан:

2.1. 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.

2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
- аппаратных и программных средств защиты.

2.3. Обеспечивать работоспособность элементов ИСПДн .

2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, документов.

2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7. Проводить периодический контроль принятых мер по защите, в пределах возложенных на него функций.

2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.

2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

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

2.15. Не допускать к работе на рабочих станциях посторонних лиц;

2.16. Осуществлять контроль монтажа оборудования специалистами сторонних организаций.

3. Резервирование и восстановление работоспособности ПО, баз данных и СЗПДн

3.1.В случае потери защищенной информации (в результате непреднамеренных и преднамеренных действий пользователей, нарушения правил эксплуатации технических средств АИС и СЗПДн, возникновения внештатных ситуаций и обстоятельств непреодолимой силы) в кратчайшие сроки, не превышающие одного рабочего дня администраторы безопасности конфиденциальной информации, в том числе ПДн, информационных систем персональных данных, резервирования и восстановления работоспособности ПО, баз данных и СЗПДн предпринимают меры по восстановлению работоспособности.

3.2.Предпринимаемые меры, по возможности, согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена с целью получения высококвалифицированной консультации в кратчайшие сроки.