УТВЕРЖДЕНО приказом
ОГПОБУ
«Политехнический
техникум»
№134 от 11.05.2016 г.

ИНСТРУКЦИЯ

администратора информационной безопасности информационных систем персональных данных в ОГПОБУ «Политехнический техникум»

1. Общие положения.

1.1. Администратор информационной безопасности назначается нормативным актом и отвечает за обеспечение устойчивой работоспособности и информационной безопасности объекта информатизации.

1.2. Администратор информационной безопасности несет ответственность за организацию работ по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники (СВТ) на объекте вычислительной техники (ОВТ) в ОГПОБУ Политехнический техникум.

2. Функции администратора информационной безопасности.

2.1. Осуществляет настройку ОВТ, при этом:

- реализует полномочия доступа для каждого пользователя к элементам защищаемых информационных на основе утвержденного руководством перечня лиц, допущенных к обработке защищаемой информации в ИСПДн;
- назначает временные пароли к информационным ресурсам.
- своевременно удаляет пользователя из базы данных при увольнении или перемещении сотрудника;
- периодически производит или организовывает смену паролей пользователями для доступа в систему обработки информации ОВТ.

Осуществляет настройку и сопровождение подсистемы регистрации и учета:

- своевременно информирует руководство о несанкционированных действиях персонала.
- проводит контроль соответствия общесистемной программной среды эталону;
- обеспечивает поддержание установленного порядка и соблюдение требований инструкции по антивирусной защите.

3. Администратор информационной безопасности обязан:

3.1. Обеспечивать функционирование и поддерживать работоспособность ИСПДн в пределах возложенных на них функций.

3.2. В случае отказа работоспособности технических средств и программного обеспечения СВТ, АРМ принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.3. Информировать руководство о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам АРМ.

4. Администратор информационной безопасности имеет право:

4.1. Контролировать работу пользователей на автоматизированных рабочих местах АРМ.

4.2. Требовать прекращения обработки информации, как в целом, так и отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования АРМ.

Подготовил:

С инструкцией ознакомлен _____ А.Л. Кириллов