

Мероприятия по информационной безопасности, обеспечивающие защиту от несанкционированного доступа к информационным ресурсам в МБОУ ДО ДЮСШ «Салют»

Осуществление мероприятий по информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам в МБОУ ДО ДЮСШ «Салют», проводится в соответствии с инструкцией «О мерах по обеспечению информационной безопасности в МБОУ ДО ДЮСШ «Салют» и включает комплекс повседневно проводимых мероприятий:

- допуск (предоставление прав доступа) к информации, средствам информатизации и в помещения;
- доступ к информации, средствам информатизации и в помещения в соответствии с предоставленными правами, ведение Журнала учета доступа;
- правильное с точки зрения информационной безопасности содержание (эксплуатация и хранение) средств информатизации;
- обеспечение безопасности информации (хранение носителей информации способом, исключающим их утрату, несанкционированное копирование и получение; хранение применяемых средств защиты информации, в том числе средств доступа к ним, способом, исключающим их несанкционированное использование).
- использование средств защиты информации, недопущение их несанкционированного применения, обеспечение их сохранности и исправности, проведение их технического обслуживания, организация ремонта в случае выхода из строя и выполнение других эксплуатационных операций, ведение Журнала учета средств информатизации.
- контроль состояния информационной безопасности (администратор сети контролирует состояние информационной безопасности в ЛВС; выполнение сотрудниками установленного порядка действий по доступу к объектам информационной системы; анализирует состояние информационной системы с целью выявления попыток несанкционированного доступа и использования средств информатизации и информации; контролирует правильность использования имеющихся коллективных и индивидуальных средств информационной защиты).
- действия в случае выявления нарушений информационной безопасности

(выявление факта нарушения; прекращение всех операций, связанных с участком, на котором произошло нарушение;
принятие экстренных мер для прекращения несанкционированного доступа или использования информации; оповещение о нарушении; восстановление работоспособности информационной системы; расследование причин нарушения информационной безопасности; проверка состояния информационной безопасности по факту нарушения).

- инструктаж по информационной безопасности (проводятся следующие виды инструктажа: вводный, периодический, разовый).