**Сведения о реализуемых в Администрации Колпашевского района требованиях к защите персональных данных**

Реализация требований к защите персональных данных от неправомерного или случайного доступа к персональным данным, их уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с персональными данными, осуществляется Администрацией Колпашевского района правовыми, организационными и техническими (программно и аппаратно реализуемыми) мерами, а также путем осуществления контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

**Правовые меры:**

Администрацией Колпашевского района разрабатываются и принимаются правовые акты, направленные на предотвращение и  защиту персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

**Организационные меры:**

назначение лица, ответственного за организацию обработки персональных данных;

распределение ответственности по вопросам защиты данных между работниками Администрации Колпашевского района;

своевременное выявление угроз безопасности данных и принятие соответствующих мер защиты;

доведение до работников Администрации Колпашевского района требований действующего законодательства по защите персональных данных.

**Технические (программно и аппаратно реализуемые) меры:**

резервное копирование информационных ресурсов;

применение прикладных программных продуктов, отвечающих требованиям защиты данных;

организация контроля доступа в помещения и здания Администрации Колпашевского района, их охрана в нерабочее время;

применение технических средств защиты, сертифицированных компетентными государственными органами (организациями) на соответствие требованиям безопасности;

оптимальная настройка операционной системы и прикладного программного обеспечения вычислительных средств, применяемых для обработки данных;

шифрование данных при передаче и хранении (криптографическая защита);

использование электронной подписи;

применение межсетевых защитных (фильтрующих) экранов;

антивирусный мониторинг и детектирование;

оборудование зданий и помещений системами безопасности (пожарной и охранной сигнализации, пожаротушения, телевизионного наблюдения и т.п.).