*Информационная справка к вопросу 2*

**Об обеспечении безопасности сведений в информационных
системах органов Администрации города Ханты-Мансийска
и муниципальных учреждений города**

В связи с регулярными изменениями в законодательстве, а также рекомендациями и указаниями регуляторов ФСТЭК, ФСБ, Роскомнадзора органам Администрации города Ханты-Мансийска и муниципальным учреждениям города необходимо своевременно соблюдать требования законодательства и исполнять рекомендации.

Должностным лицам, ответственным за информационную безопасность, требуется регулярно вносить изменения во внутренние нормативные правовые акты, проходить курсы повышения квалификации, организовывать установку и настройку технических средств и программного обеспечения защиты информации.

 В целях предотвращения реализации угроз безопасности информации
в органах Администрации города Ханты-Мансийска и муниципальных учреждений необходимо принимать дополнительные меры по защите информации. Так для предотвращения возможности использования систем удаленного доступа для реализации угроз безопасности информации следует ограничить доступ к системам удаленного доступа из сети Интернет, на регулярной основе проводить резервное копирование баз данных на съемные носители.

 Актуальную информацию, связанную с информационной безопасностью можно найти на официальных сайтах регуляторов ФСБ, ФСТЭК, Роскомнадзор, на специализированных семинарах, вебинарах
и курсах повышения квалификации.

Ответственным за информационную безопасность должностным лицам органов Администрации города Ханты-Мансийска и муниципальных учреждений, необходимо проводить разъяснения о запрете на запуск подозрительных вложений, переходе по сомнительным ссылкам
и незамедлительное информирование администратора безопасности
о подозрительных электронных письмах (вложениях).

Вместе с тем необходимо установить запрет (под роспись сотрудников):

на использование на рабочих автоматизированных местах личных съемных носителей (флешек, съемных жестких дисков, подключение мобильных телефонов), а также на использование общедоступных облачных хранилищ и личной электронной почты;

на использование видеоконференций с рабочего места иностранных компаний (zoom, skype и т.д);

исключить подключение к удаленным рабочим местам (в том числе для администрирования и обновления программного обеспечения) с помощью иностранного программного обеспечения (AmmyAdmin, Teamviewer и т.д.).

При этом, для организации удаленного доступа к Автоматизированному рабочему месту, допускается использование удаленного помощника
«Мой Ассистент».