

Памятка по информационной безопасности сотрудникам администрации города Владимира

Парольная защита

Сохраняйте в тайне личные пароли. Никогда не сообщайте пароль другим лицам, и не храните записанный пароль в общедоступных местах.

Не используйте пароль доступа, выданный администрацией в других программах и на сайтах, где требуется регистрация.

Используйте только надежные пароли - длиной от 8 символов, включающие заглавные, строчные буквы, цифры.

Регулярно обновляйте пароли. Не используйте один и тот же пароль для разных сервисов

Антивирусная защита

Никогда не отключайте установленное на АРМ антивирусное программное обеспечение.

Обязательно проверяйте на наличие вирусов все носители информации (диски, флешки и т.п.).

Во всех случаях возможного проявления действия вирусов или подозрении на наличие вируса не пытайтесь удалить вирус самостоятельно, незамедлительно сообщите об этом штатному специалисту.

Интернет и электронная почта

Все файлы, загружаемые из Интернета и вложения электронной почты обязательно проверяйте на отсутствие вирусов с помощью антивирусного ПО.

Не переходите по ссылкам, не запускайте программы и не открывайте файлы, полученные по электронной почте и в мессенджерах от неизвестного Вам отправителя.

Не передавайте по электронной почте и по другим каналам Ваши пароли, персональные данные, конфиденциальную и секретную информацию.

Не принимайте никаких соглашений при посещении сайтов, смысла которых Вы не понимаете.

Прочее

Не устанавливайте самостоятельно программное обеспечение, если это не входит в Ваши обязанности.

Запрещается устанавливать и запускать нелицензионное или не относящееся к выполнению Ваших должностных обязанностей программное обеспечение.

Не допускайте посторонних лиц к работе на АРМ.

При временном оставлении рабочего места в течение рабочего дня в обязательном порядке блокируйте компьютер.

Помните, высокие результаты достижения информационной безопасности могут быть достигнуты только усилиями всех сотрудников!