УТВЕРЖДАЮ

ВрИО директора МБУ ДО

«ДЮСШ г.Пошехонье»

/М.А.Тутынин/

(Подпись) (Ф.И.О.)

Приказ №10/1

«07» 02 2020 г.

Приложение № 5

Памятка пользователю по информационной безопасности

Парольная защита

- ✓ Никогда не сохраняйте ваши пароли в программах. Большинство программ хранят их в открытом виде и тот, кто получит доступ к вашему компьютеру, получит доступ и к ним.
- ✓ Сохраняйте в тайне личный пароль. Никогда не сообщайте пароль другим лицам, и не храните записанный пароль в общедоступных местах.
- ✓ В случае производственной необходимости (командировка, отпуск и т.п.), при проведении проверочных мероприятий, выполняемых отделом по защите информации, работ, проводимых отделом информационных технологий и требующих знания пароля пользователя, допускается раскрытие значений своего пароля начальникам этих подразделений. По окончанию производственных, или проверочных работ работники самостоятельно производят немедленную смену значений "раскрытых" паролей.
- ✓ Не используйте пароль доступа в локальную сеть МБУ ДО «ДЮСШ г.Пошехонье» в других программах и на сайтах, где требуется регистрация;
- ✓ Следует помнить, что для печати документов на принтере, подключенном к другому компьютеру, не требуется знать пароль от этого компьютера. Достаточно включить компьютер, к которому присоединен нужный принтер, дождаться приглашения: «Нажмите Ctrl+Alt+Del для входа в систему». После появления приглашения можно осуществлять печать. Для выключения компьютера нужно нажать кнопку «Завершить работу» не вводя пароль.

Антивирусная защита

- ✓ Никогда не отключайте установленное на АРМ антивирусное программное обеспечение.
- ✓ Обязательно проверяйте на наличие вирусов все внешние носители информации (дискеты, диски, флешки и т.п.), поступающие со стороны (из внешних организаций, других подразделений ОУ и т.п.)
- ✓ Во всех случаях возможного проявления действия вирусов или подозрении на наличие вируса не пытайтесь удалить вирус самостоятельно, незамедлительно сообщите об этом ответственному за антивирусный контроль и оцените с ним возможные пути заражения и распространения данного вируса.

Интернет и электронная почта

- ✓ Содержание Интернет-ресурсов, а также файлы, загружаемые из Интернета, обязательно проверяйте на отсутствие вредоносных программ и вирусов.
- ✓ Не переходите по ссылкам, не запускайте программы и не открывайте файлы, полученные по электронной почте от неизвестного Вам отправителя.
- ✓ Не передавать по электронной почте Ваши пароли.
- ✓ 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;
- ✓ Располагайте мониторы и печатающие устройства таким образом, чтобы исключить несанкционированный доступ к отображаемой и печатаемой информации.
- ✓ При временном оставлении рабочего места в течение рабочего дня в обязательном порядке блокируйте компьютер нажатием комбинации клавиш «Win + L».