Требования к среде функционирования АРМ:

1. На АРМ сотрудника должна быть установлена только одна лицензионная ОС (целевая ОС - Windows 10 с последними обновлениями безопасности).

2. Должна быть установлена "заплатка" по отмене перехода на зимнее время (KB2998527).

3. Должна быть настроена синхронизация с сервером времени (http://help.tatar.ru/ -> Портал пользователей).

4. Должна быть настроена синхронизация с DNS-серверами ГИСТа (http://help.tatar.ru/ -> Портал пользователей).

5. Должна быть установлена библиотека компонентов Microsoft Visual C++ 2015 Redistributable - 14.0.23026 (vc_redist.x86.exe или vc_redist.x64.exe).

6. Должна быть установлена сертифицированная ФСТЭК версия антивирусного ПО Kaspersky Endpoint Security 11 для Windows 11.3.0.773 (для рабочих станций и файловых серверов) с актуализированными базами обновлений и актуальной лицензией (http://help.tatar.ru/ -> Портал пользователей -> Антивирусная защита).

7. Должна быть отключена учетная запись для гостевого входа Guest.

8. Должны переименовать стандартную учетную запись Administrator и установить надежный пароль в соответствии с парольной политикой, см. п.9.

9. Для входа в BIOS, ОС, ПО АРМ должны использоваться учетные записи, которым заданы пароли в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (USER, ADMIN и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;
- запрещается записывать пароли на материальные носители и хранить их в легкодоступных местах, в том числе на мониторе, рабочем столе или ящиках стола;
- периодичность смены пароля не должна превышать 6 месяцев.

10. Необходимо определить в BIOS установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM, исключаются прочие нестандартные виды загрузки ОС, включая сетевую загрузку.

11. **Администратор безопасности, а также Пользователи несут персональную ответственность за обеспечение режима конфиденциальности в отношении паролей доступа. Пароль должен быть изменен раньше плановой замены в случае его компрометации.**