Приложение №3
к приказу ГАУЗ ТО
«Городская поликлиника №6»
от 26.01.24 № 35

Инструкция
по обеспечению информационной безопасности при работе пользователей с информационными системами ГАУЗ ТО «Городская поликлиника №6»

Информационные ресурсы, хранящиеся в электронном виде в информационных системах (далее - ИС) Учреждения на магнитных, оптических и иных носителях информации, являются собственностью ГАУЗ ТО «Городская поликлиника №6». Все без исключения работники Учреждения, а также представители внешних организаций, допущенные к данным информационным ресурсам и участвующие в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющие доступ к аппаратным средствам, программному обеспечению и данным автоматизированной системы (далее - пользователи), несут персональную ответственность за свои действия.

Пользователи **обязаны:**

1. использовать информационные ресурсы предприятия только для выполнения своих функциональных обязанностей в соответствии с положением о структурном подразделении, своими должностными инструкциями;
2. строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС;
3. знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции;
4. хранить в тайне свой пароль (пароли), с установленной периодичностью менять свой пароль (пароли);
5. выполнять требования по антивирусной защите в ИС в части, касающейся действий пользователей рабочих станций[1] (далее - РС) ИС;
6. присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним РС;
7. немедленно вызывать администратора безопасности (ответственного за соблюдение информационной безопасности ГАУЗ ТО «Городская поликлиника №6») и ставить в известность руководителя подразделения в следующих случаях:

а) нарушения целостности пломб, наклеек, нарушения или несоответствия номеров печатей на аппаратных средствах РС или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищенной РС;

---

[1] Рабочая станция - персональный компьютер пользователя ИС, включающий в свой состав системный блок, монитор, клавиатуру, оптический манипулятор, набор программного обеспечения. Дополнительно может комплектоваться другими периферийными устройствами

б) несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств РС;

в) отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию РС, выхода из строя или неустойчивого функционирования узлов РС или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

г) некорректного функционирования установленных на РС технических средств защиты;

д) обнаружения непредусмотренных кабельных отводов и устройств, подключенных к РС.

Пользователям **запрещается:**

1. использовать компоненты программного и аппаратного обеспечения ИС Учреждения в неслужебных целях;
2. самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств РС или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные конфигурациями рабочих станций;
3. самовольно производить сборку, разборку, установку и техническое обслуживание аппаратных средств;
4. осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
5. записывать и хранить информацию, являющуюся конфиденциальной, на неучтенных носителях информации (гибких магнитных дисках, оптических дисках, флэш-картах и т.п.);
6. оставлять включенной без присмотра свою РС, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана);
7. отключать средства защиты и использовать не согласованные с администратором безопасности режимы их функционирования;
8. осуществлять поиск способов преодоления установленной аппаратно - программной защиты информации, а также использовать аппаратно - программные средства, реализующие названные способы;
9. разглашать информацию, открывающую доступ для других лиц к техническим средствам и данным или передавать кому-либо средства доступа к ним;
10. умышленно использовать недокументированные особенности и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок пользователи обязаны ставить в известность администратора безопасности (ответственного за безопасность информации) и руководителя своего структурного подразделения.