

Инструкция о предоставлении прав доступа к защищаемым информационным ресурсам ГАУЗ ТО «Городская поликлиника №6»

Настоящая инструкция регламентирует порядок предоставления сотрудниками Учреждения прав доступа к информационным системам, подлежащим защите.

Каждому сотруднику, допущенному к работе с конкретной информационной системой (далее - ИС) ГАУЗ ТО «Городская поликлиника №6» предоставляется персональное уникальное имя (логин, учетная запись), под которым он регистрируется и получает доступ к ресурсам ИС. Авторизация пользователя в информационной системе может осуществляться, как с полномочиями учетной записи домена, так и дополнительных учетных записей для каждой ИС.

Не допускается использование несколькими работниками одного и то же имени пользователя при работе с ИС, передача кому-либо своих учетных записей, а также работа с ИС с использованием чужих учетных записей.

Регистрация работника и предоставление ему прав доступа для работы в информационной системе производится по письменному заявлению руководителя структурного подразделения, в котором работает данный работник.

На основании согласованного заявления ответственный администратор ИС заводит данные пользователя в систему.

Учетные записи всех пользователей должны быть «привязаны» к конкретным рабочим станциям (MAC - адресам их сетевых карт) или к сегменту (группе) рабочих станций.

Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в квартал.

Централизованный учет сведений о защищаемых ресурсах ведет администратор вычислительных сетей ГАУЗ ТО «Городская поликлиника №6».

Инструкция по организации парольной защиты информационных систем и рабочих станций пользователей ГАУЗ ТО «Городская поликлиника №6»

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах ГАУЗ ТО «Городская поликлиника №6», а также контроль действий пользователей и обслуживающего персонала системы при работе с паролями.

1. Требования к генерации паролей:
 - обязательная длина пароля – не менее - 6 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, цифровые значения даты рождения и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, TESTи т.п.);
 - при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;
 - личный пароль пользователь не имеет права сообщать никому, в том числе администратору информационной системы;
 - длина пароля администратора информационной системы должна быть не менее 10 символов.
2. Пароли административного доступа к телекоммуникационному оборудованию, входящему в состав КСПД генерируются централизованно.
3. Плановая смена паролей администраторов и пользователей должна проводиться регулярно, не реже одного раза в квартал.
4. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на работу в другое подразделение организации и т.п.) должна производиться администраторами немедленно после окончания последнего сеанса работы данного пользователя с системой.
5. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на работу в другое подразделение организации со снятием соответствующих обязанностей др.) администраторов или других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем автоматизированной системы ГАУЗ ТО «Городская поликлиника №6».

6. Хранение сотрудником значений своих паролей на бумажном носителе, либо записанные иным доступным способом, позволяющим их прочесть не допускается.

7. Контроль за действиями пользователей по парольной защите возлагается на администратора вычислительных сетей ГАУЗ ТО «Городская поликлиника №6».