Приложение к приказу № 4-06 от 04.07.24

УТВЕРЖДАЮ

Главный врач

ГБУ РД «Республиканская клиническая

больница им. А.В. Вишневского»

Мусаев Г. Х. _____

«04» июля 20 24 г.

ПОЛОЖЕНИЕ
по организации парольной защиты
по ГБУ РД «Республиканская клиническая больница им. А.В. Вишневского»

ОБЩИЕ ПОЛОЖЕНИЯ

1. Парольная защита доступа к эксплуатируемым вычислительным ресурсам и информационным системам устанавливается в целях недопущения утечки данных, а также их несанкционированной модификации или уничтожения.

2. Настоящее положение регламентирует организационно-техническое обеспечение процессов генерации и смены паролей от всех эксплуатируемых вычислительных ресурсов и информационных систем, меры обеспечения безопасности при использовании паролей, а также контроль за действиями сотрудников ГБУ РД «Республиканская клиническая больница им. А.В. Вишневского» при работе с паролями.

3. Требования настоящего положения распространяются на всех сотрудников ГБУ РД «Республиканская клиническая больница им. А.В. Вишневского» (далее – сотрудники) и должны применяться для всех средств эксплуатируемой вычислительной техники.

4. Контроль за действиями сотрудников при работе с паролями возлагается на начальника отдела по защите информации.

ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

5. При первом входе в систему сотрудник должен заменить пароль однократного доступа на самостоятельно сгенерированный пароль.

6. Сотрудники обязаны менять пароль не реже одного раза в 60 дней, а также внепланово по требованию начальника отдела по защите информации.

7. При смене административных паролей на доступ к эксплуатируемым вычислительным ресурсам и информационным системам, сотрудники обязаны передавать начальнику отдела по защите информации новые пароли в отдельном конверте, исключающем возможность увидеть пароль через конверт, например, путем просвечивания конверта ярким светом. На конверте необходимо указать перечень вычислительных ресурсов и систем, пароли от которых находятся внутри, адрес их расположения, поставить подпись сотрудника и дату запечатывания конверта.

8. Конверты должны храниться в кабинете начальника отдела по защите информации, ежемесячно проверяться на наличие и целостность.

9. При получении конверта с обновленными паролями начальник отдела по защите информации должен уничтожить конверт с устаревшими паролями способами, исключающими возможность последующего восстановления информации.

10. В случае вскрытия либо использования конвертов с паролями, по окончании выполнения работ необходимо произвести работы по созданию новых паролей с последующим запечатыванием конверта с новыми паролями в соответствии с пунктом 7.

11. В случае использования пароля сотрудника во время его отсутствия на рабочем месте (в случае возникновении нештатных ситуаций, форс-мажорных

обстоятельств и т. п.) начальник отдела по защите информации должен произвести внеплановую смену личного пароля сотрудника после проведенных работ.

12. В случае утраты или компрометации пароля сотрудник обязан обратиться к начальнику отдела по защите информации. Начальник отдела по защите информации должен предпринять меры по срочной (внеплановой) смене пароля.

13. Сотрудникам запрещается:

13.1. сообщать посторонним лицам пароль для доступа к эксплуатируемым вычислительным ресурсам и информационным системам;

13.2. осуществлять ввод пароля для доступа в систему в присутствии посторонних лиц;

13.3. записывать пароли в общедоступных местах (монитор, обратная сторона клавиатуры, отдельные листы бумаги и т.д.);

13.4. использовать повторно ранее использованные пароли;

13.5. в настройках учетной записи создавать подсказки для паролей;

13.6. создавать одинаковые (или идентичные) пароли для учетных записей, используемых в разных информационных системах.

14. В случае увольнения сотрудника, перехода в другое структурное подразделение больницы, либо в случае длительного отпуска сотрудника специалистами отдела кадров организации доводится вышеуказанная информация до специалистов по защите информации в целях блокировки учетной записи пользователя.

15. Ознакомление всех сотрудников, использующих средства вычислительной техники, с требованиями настоящего положения проводит отдел по защите информации.

ТРЕБОВАНИЯ К ПАРОЛЯМ

16. Для минимизации угроз, связанных с возможностью внутреннего и внешнего подбора паролей, используемых для аутентификации пользователей и администраторов на объектах организации предъявляются следующие требовани:

16.1. Пароль не должен включать в себя название учетной записи пользователя или содержать отдельные его части длиной больше двух символов;

16.2. пароль должен состоять не менее чем из восьми символов;

16.3. для формирования паролей использовать алфавит, состоящий как минимум из строчных и прописных символов латинского алфавита, цифр и специальных символов ((@, #, $, &, *, % и т. п.);

16.4. пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, клички домашних животных, наименования ПЭВМ, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.)), а также другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;

16.5. не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

16.6. не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

16.7. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

17. В зависимости от типа информационной системы и его класса (ГИС, ИСПДн, КИИ) к объекту IT-инфраструктуры организации могут применяться дополнительные требования по защите информации (в том числе и требования к парольной политике). Ознакомление пользователей таких систем с дополнительными требованиями к парольной политике производит начальник отдела по защите информации. Если на таких объектах применяются сертифицированные ФСБ России и/или ФСТЭК России средства защиты информации от несанкционированного доступа, начальник отдела по защите информации должен ознакомить пользователя с инструкцией по работе со средством защиты информации.

РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ СРЕДСТВ ПАРОЛЬНОЙ ЗАЩИТЫ

18. Для минимизации угроз, связанных с возможностью внутреннего и внешнего злоумышленников по подбору паролей, используемых для аутентификации пользователей и администраторов на объектах IT-инфраструктуры организации, при настройке средств парольной защиты целесообразно обеспечить:

18.1. настройку механизмов защиты от подбора аутентификационных данных. Использовать меры по временной блокировке учетных записей;

18.2. хранение аутентификационных данных только в криптографически защищенном виде или в запечатанном конверте.

ТРЕБОВАНИЯ К НАСТРОЙКАМ БЕЗОПАСНОСТИ ЭКСПЛУАТИРУЕМЫХ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ И ИНФОРМАЦИОННЫХ СИСТЕМ

19. Учетная запись пользователя должна блокироваться после 4 неверных попыток доступа не менее, чем на 15 минут.

20. Сотрудникам запрещается использовать возможность запоминания пароля средствами операционной системы либо прикладного программного обеспечения.

ОТВЕТСТВЕННОСТЬ

21. Сотрудники несут персональную ответственность за использование паролей, не соответствующих вышеперечисленным требованиям, а также за их разглашение.