Утверждаю
И.о. начальника ГБУ РО «МИАЦ»
_____С.А. Жиляков
«21» апреля 2022 года

Парольная политика
в государственном бюджетном учреждении Ростовской области «Медицинский информационно-аналитический центр» (ГБУ РО «МИАЦ»)

1. Парольная политика представляет собой свод правил, рекомендаций и ограничений по предоставлению сотрудникам учреждения и другим лицам доступа к информационным системам ГБУ РО «МИАЦ», а также к специализированным программным ресурсам (далее – ИС МИАЦ).

2. Для входа в ИС МИАЦ используется учетная запись, позволяющая однозначно определить кто осуществляет действия в информационной системе. Учетная запись состоит из логина и пароля.

Формирование и выдачу учетных записей для ИС МИАЦ осуществляют руководители структурных подразделений ГБУ РО «МИАЦ», которые данные ресурсы администрируют.

Выдача учетной записи производится только лично, после проверки документа, удостоверяющего личность получателя, и доверенности, идентифицирующей получателя как сотрудника организации, заверенной руководителем организации (для внешних пользователей). За выдачу учетной записи получатель ставит свою подпись в соответствующих регистрационных документах (для всех пользователей).

Срок выдачи учетной записи – не более трех рабочих дней с момента получения заявки.

3. Логин пользователя является открытой информацией.

Процедура формирования логинов для внутренних и внешних пользователей различается.

3.1. Логин для постоянного доступа в ИС МИАЦ для внутренних пользователей (физических лиц) составляется следующим образом: первые три буквы фамилии в «транслите» латинскими буквами в нижнем регистре, затем нижнее подчеркивание «_», потом первая буква имени в нижнем регистре (abc_a). Если происходит совпадение с уже зарегистрированным логином, то после первой буквы имени добавляется следующая буква и т. д. (abc_ab). При полном совпадении фамилии, имени и отчества пользователей после букв фамилии и имени добавлять порядковый номер (abc_a1). В случае

смены пользователем информационной системы, фамилии или имени, логин для доступа остается неизменным.

Логином для временного доступа (для тестирования ресурсов системы, проведения обучающих мероприятий и иных краткосрочных действий в системе, а также для предоставления доступа к ресурсам системы на строго определенный срок) являются логины: «test» – тестовый (для тестирования ресурсов системы) и «temp» – временный (для временных целей).

3.2. Логин для постоянного доступа в ИС МИАЦ для внешних пользователей (юридических лиц) составляется следующим образом: первые буквы в «транслите» латинскими буквами в нижнем регистре в соответствии с Приложением № 1, затем нижнее подчеркивание «_», потом цифра – порядковый номер пользователя данной организации (cgb_aaa_1).

3.3. Ранее выданные логины остаются без изменений и выводятся из информационных систем по мере необходимости и актуальности.

4. Пароль является закрытой информацией и должен быть известен только пользователю (владельцу логина).

Для первичного входа в ИС МИАЦ администратором соответствующей информационной системы генерируется временный пароль, состоящий: в «транслите» латинскими буквами в нижнем регистре слово «miac» и затем без пробелов и точек дата создания учетной записи (miac190422). Временный пароль меняется пользователем сразу же после первичного входа на постоянный пароль.

В случае технической невозможности информационной системы автоматической смены временного пароля на постоянный, администратором соответствующей ИС МИАЦ генерируется постоянный пароль в соответствии с пунктом 5 и выдается вышеуказанным порядком определенным в пункте 2.

Администраторам ИС МИАЦ запрещено хранить пароли пользователей.

Ранее сформированные пароли остаются без изменений и выводятся из информационных систем по мере необходимости и актуальности.

5. Порядок обращения пользователей с парольной информацией для предотвращения несанкционированного доступа к своему автоматизированному рабочему месту:

– забывать или терять пароль крайне недопустимо, пользователь несет персональную ответственность за его сохранность и конфиденциальность;

– не использовать простые пароли, например: «12345, 123qwe321, 10121980 и т.п.»;

– длина пароля должна быть не менее 8 символов;

– в числе символов пароли должны обязательно содержать прописные и строчные буквы (a-z, A-Z), то есть в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);

– не использовать личные пароли (от социальных сетей, личной электронной почты и т. д.) для служебных программ (1С, сервер) и наоборот, не использовать служебные пароли для личных целей;

– не сохранять пароли в программах или браузере для интернет-банков, личных кабинетах платежных систем и других сервисов с вашими или чужими данными, содержащими конфиденциальную информацию (персональные данные сотрудников или коммерческую тайну организации);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

– периодичность смены пароля не должна превышать 90 календарных дней;

– пароли запрещено сообщать любым лицам, передавать другим пользователям или техническим специалистам (администраторам), за исключением описанных выше случаев;

– хранить записанный пароль в общедоступных местах, в том числе на мониторе, клавиатуре и т.п.

6. В случае если пользователь утерял, забыл или по мнению администраторов ИС МИАЦ любым общеизвестным способом скомпрометировал свой пароль доступа в информационную систему, либо сотрудники отдела защиты информации ГБУ РО «МИАЦ» обнаружили любые несанкционированные действия с учетной записью пользователя или порядком обращения с парольной информацией – пароль пользователя аннулируется, учетная запись блокируется и производится доклад о данном инциденте в адрес заместителя начальника ГБУ РО «МИАЦ» по информатике.

7. Большинство программ хранит пароли в открытом доступе. Посторонний виртуальный или физический доступ к автоматизированному рабочему месту, а также вирусное вторжение способны, соответственно, предоставить доступ к парольной информации пользователей.

Пользователь автоматизированного рабочего места при исполнении своего должностного функционала обязан соблюдать следующие требования по обеспечения сохранности парольной информации:

– не запускать программное обеспечение не относящееся

к выполнению должностных обязанностей;

– при временном оставлении рабочего места в течение рабочего дня в обязательном порядке блокировать рабочее место нажатием комбинации клавиш «Win+L»;

– производить сканирование средствами антивирусной защиты всех вложений к электронным письмам или полученных через мессенджеры файлов и документов на наличие вредоносного содержимого, даже если файлы (документы) доставлены от легитимного адресата;

– в случае некорректной работы антивирусной программы (появление восклицательного знака или крестика на иконке, получения сообщения об отключении антивирусной программы и т. д.) немедленно сообщить об этом начальнику отдела защиты информации ГБУ РО «МИАЦ»;

– не нажимать на ссылки из письма, если они заменены на слова, не наводить на них мышкой и не просматривать полный адрес сайтов;

– не открывать вложения к письмам, особенно если в них содержатся документы с макросами, архивы с паролями;

– внимательно относиться к письмам на иностранном языке, адресованным большому количеству адресатов;

– не открывать содержимое электронных писем, в которых содержатся призывы к действиям с применением глаголов в повелительном наклонении: «Открой», «Прочитай», «Ознакомься» и т.д., а также с темами письма про финансы, банки, геополитическую обстановку или угрозы безопасности;

– не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или короткие (сервисы сокращения ссылок: bit.ly, bit.do, tinyurl.com и т.д.) или получены от неизвестных отправителей;

– при получении подозрительного электронного письма, сообщения, файла, документа – не открывать вложение самостоятельно, сообщить о данном факте начальнику отдела защиты информации ГБУ РО «МИАЦ».

Заместитель начальника ГБУ РО «МИАЦ»
по информатике В.С. Чистяков