Министерство труда и социальной защиты Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«НОВОКУЗНЕЦКИЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЦЕНТР
МЕДИКО-СОЦИАЛЬНОЙ ЭКСПЕРТИЗЫ И РЕАБИЛИТАЦИИ ИНВАЛИДОВ»
МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
(ФГБУ ННПЦ МСЭ и РИ Минтруда России)

П Р И К А З

21.12.2023 г. № 867/К

О парольной защите в
информационных системах «1С»

В соответствии с Федеральными Законами Российской Федерации от 08.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 06.12.2011 № 402-ФЗ «О бухгалтерском учете», от 27.07.2006 № 152-ФЗ «О персональных данных»

п р и к а з ы в а ю:

1. Обеспечить настройку политики парольной защиты в информационных системах «1С:Бухгалтерия государственного учреждения» и «1С:Зарплата и кадры государственного учреждения» до 22.01.2024 г.

Ответственный исполнитель: ведущий программист А.А. Кошаров.

2. Назначить ответственным лицом за выдачу временных паролей, соблюдение порядка их смены, хранения и использования, ведущего программиста А.А. Кошарова.

3. На период ежегодного отпуска, больничного листа и т.п. ответственных лиц, функциональные обязанности возлагаются на лиц их замещающих.

4. Утвердить Регламент выдачи паролей доступа администратором информационной безопасности и хранения паролей пользователями информационных систем (Приложение № 1).

5. Канцелярии ФГБУ ННПЦ МСЭ и РИ Минтруда России ознакомить работников, указанных в Приложении № 2 с настоящим приказом в течение 14-ти рабочих дней после его подписания, а также с утвержденным Регламентом выдачи паролей доступа администратором информационной безопасности и хранения паролей пользователями информационных систем под подпись.

Ответственный исполнитель: заведующий канцелярией Л.В. Гаева.

6. Контроль за исполнением настоящего приказа возложить на заведующего ЛАСУ – А.А. Гаева.

И.о. генерального директора Е.М. Васильченко

Приложение № 1
Утверждено приказом
от 21.12.2023 № 867/К

РЕГЛАМЕНТ

выдачи паролей доступа администратором информационной безопасности и хранения паролей пользователями информационных систем в ФГБУ ННПЦ МСЭ и РИ Минтруда России

Настоящий Регламент выдачи и хранения паролей в Федеральном государственном бюджетном учреждении «Новокузнецкий научно-практический центр медико-социальной экспертизы и реабилитации инвалидов» Министерства труда и социальной защиты Российской Федерации (далее – Регламент и Учреждение соответственно) разработан в целях установления общих правил, единых требований и процедур к управлению средствами аутентификации при организации парольной защиты автоматизированных рабочих мест работников Учреждения и в информационных системах.

1.2. Регламент разработан в соответствии со следующими документами:

– Федеральным законом от 08.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
– Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
– Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
– приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
– приказом Федеральной службы по техническому и экспортному контролю от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
– Национальным стандартом Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
– Методическим документом Федеральной службы по техническому и экспортному контролю «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11.02.2014).

– Регламентом парольной защиты в информационных системах Учреждения утвержденном приказом от 01.03.2021 г. № 152/К.

1.3. Регламент предназначен для работников Учреждения, ответственных за эксплуатацию и администрирование информационных систем и ресурсов, за обеспечение информационной безопасности, а также работников Учреждения, использующих информационные ресурсы и системы Учреждения.

1.4. Регламент устанавливает основные этапы деятельности:

– по защите доступа к автоматизированным рабочим местам работников и информационным системам Учреждения с использованием паролей;

– по определению требований к энтропии, сложности используемых паролей, сроку их действия и процедуре их смены;

– по определению ответственности работников Учреждения за нарушения при организации парольной защиты.

2. Используемые в Регламенте термины и определения

2.1. Защита паролем – это метод управления доступом, при котором получить доступ к информационному ресурсу, войти в информационную систему можно только с помощью правильных учетных данных, позволяющий обезопасить информацию от действий злоумышленников.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационный ресурс – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и/или правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Пароль – условное слово или произвольный набор знаков, состоящий из букв, цифр и других символов и предназначенный для подтверждения личности или полномочий.

Системы – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления Учреждения.

Система защиты информации – совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Учётная запись (аккаунт) пользователя – это хранимая в системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации), для идентификации пользователя при подключении к системе, а также содержащая информацию для авторизации и учёта.

3. Требования к генерации паролей

3.1. Управление средствами аутентификации осуществляется с помощью встроенных механизмов обеспечения информационной безопасности операционных систем, прикладного программного обеспечения информационных систем, активного сетевого оборудования, программируемых логических контроллеров и т.п. Используемые механизмы и системы: службы каталога, системы управления жизненным циклом сертификатов открытого ключа, средства защиты информации от несанкционированного доступа, системы управления доступом прикладного программного обеспечения информационных систем и активного оборудования.

3.2. Генерация паролей осуществляется следующими методами:

– автоматизировано, по правилам, заданным в информационной системе, утилитой генерации случайных паролей;

– администратором, по правилам, заданным в информационной системе;

– самостоятельно работником Учреждения при работе с информационной системой.

3.3. Пароль, заданный производителем оборудования, либо переданный пользователю администратором информационной безопасности, должен быть изменен пользователем при первом входе в информационную систему.

3.4. При использовании в информационной системе механизмов аутентификации на основе пароля (иной последовательности символов, используемой для аутентификации) или применения пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны быть следующими:

– минимальная длина парольной фразы для непривилегированных пользователей информационных систем – 8 символов;

– минимальная длина парольной фразы для пользователей с правами администратора информационных систем – 12 символов;

– алфавит пароля – не менее 30 символов (используются цифры, буквы латинского и кириллического алфавитов в верхнем и нижнем регистрах, специальные символы);

– максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 3 попытки;

– блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации на период не менее 15 минут;

– максимальный срок действия пароля – не более чем 180 дней для пользователей, не более чем 90 дней – для пользователей, обладающих повышенными полномочиями в информационных системах. Повторное использование идентификатора пользователя исключается в течение одного года.

3.5. При генерации паролей запрещается использовать общепринятые сокращения и легко вычисляемые комбинации символов, связанные с информацией о пользователе (фамилию, имя, дату рождения, наименование Учреждения и т.п.).

3.6. Не рекомендуется использовать последовательности из символов, расположенных рядом на клавиатуре, а также повторяющиеся комбинации символов.

3.7. В случае производственной необходимости пользователю информационной системы могут быть присвоены несколько учетных записей.

3.8. Использование несколькими работниками Учреждения одного и того же имени пользователя (группового имени) запрещается.

3.9. При изменении должностных обязанностей работника, связанных с переводом в другое подразделение, переводом на другую должность и т.п., учетная запись пользователя подлежит изменению (корректировке), при этом старые полномочия аннулируются.

При увольнении работника прекращение действия учетной записи и пароля осуществляется путем смены пароля и отключения (при невозможности отключения – удаления) учетной записи такого работника в службе каталогов и во всех информационных системах, куда работнику ранее был предоставлен доступ. Рекомендуемый срок хранения отключенной учетной записи – от 6 до 36 месяцев. Запрещается передавать пароль перемещенного работника иному работнику.

4. Правила использования и хранения паролей

4.1. Пароль к информационной системе, автоматизированному рабочему месту является конфиденциальной информацией и должен быть известен только работнику. Работник лично несет ответственность за конфиденциальность выданного ему администратором информационной безопасности пароля или сгенерированного им пароля.

4.2. Работник должен знать пароль доступа к автоматизированному рабочему месту и/или информационной системе наизусть. Запрещается хранить пароли в записанном виде на рабочем месте, в том числе на предметах мебели и деталях компьютера или иных приборах. Допускается хранение паролей, записанных на материальный носитель, в запирающихся на индивидуальный ключ ящиках мебели, металлических шкафах и сейфах.

4.3. Не рекомендуется хранить пароли в памяти мобильного телефона, планшета и на иных электронных носителях информации.

4.4. Ввод парольной фразы на клавиатуре должен исключать возможность наблюдения за процессом другими пользователями и/или посторонними лицами.

4.5. Запрещается передача пароля другим работникам, включая непосредственных руководителей, а также работа другого работника на автоматизированном рабочем месте или в информационной системе под паролем предыдущего пользователя, осуществившего вход в систему под своим паролем.

4.6. При подозрении на компрометацию пароля работник обязан немедленно сообщить непосредственному руководителю и работнику структурного подразделения, ответственному за информационную безопасность. При наличии технической возможности работник должен самостоятельно в кратчайший срок изменить пароль средствами операционной системы (информационной системы).

4.7. При подозрении на компрометацию пароля пользователя администратором информационной безопасности Учреждения осуществляется временная блокировка учетной записи и (по возможности) уведомление пользователя о необходимости изменения пароля.

4.8. При хранении паролей в информационной системе принимаются все возможные меры по предотвращению несанкционированного доступа к базе паролей. Рекомендуется хранение паролей в зашифрованном виде.

4.9. В информационных системах реализуется контроль подбора паролей. Количество неудачных попыток ввода неверного пароля, после которого доступ к информационной системе для данной учетной записи автоматически блокируется, не превышает трех.

5. Правила смены, прекращения и восстановления паролей

5.1. Контроль срока действия пароля осуществляется автоматически средствами информационной системы, а при отсутствии технической возможности – администратором информационной безопасности.

5.2. В информационных системах при замене пароля реализуется автоматическая проверка пароля на соответствие минимальным требованиям стойкости, указанным в разделе 3 настоящего Регламента. При отсутствии

технической возможности контроль за стойкостью паролей возлагается на администратора информационной безопасности.

5.3. В случае если работник забыл свой пароль доступа к информационной системе, он обязан обратиться к администратору информационной безопасности посредством личного визита или телефонной связи. В случае если сообщение о том, что пароль забыт, поступило посредством электронного письма (служебной записки), администратор информационной безопасности обязан связаться с работником для подтверждения информации.

5.4. Восстановление пароля осуществляется исключительно путем генерирования нового пароля.

5.5. При смене пароля выполняются следующие требования:

– новое значение пароля не должно совпадать с двумя предыдущими значениями паролей данного пользователя;

– набор символов нового пароля должен отличаться от предыдущего не менее чем на 4;

– новый пароль не должен содержать фрагментов старого пароля длиной два и более символов, расположенных на тех же позициях, что и в старом пароле.

5.6. Все изменения в правах доступа выполняются администраторами информационной безопасности не позднее трех суток с момента получения заявки на внесение изменений.

5.7. Администратором информационной безопасности локальным нормативным актом может быть введен режим блокирования учетных записей на время отпусков работников.

6. Ответственность за исполнение настоящего Регламента

6.1. Работники Учреждения несут персональную ответственность за правонарушения, совершенные в процессе осуществления своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации, и за ненадлежащее исполнение или неисполнение требований, предусмотренных Регламентом в пределах, определенных действующим трудовым законодательством Российской Федерации.

7. Внесение изменений в Регламент

7.1. Внесение изменений и дополнений в настоящий Регламент осуществляется путем утверждения его в новой редакции или путем издания приказа Учреждения о внесении изменений и дополнений в настоящий Регламент.

8. Публикация Регламента

8.1. Настоящий Регламент размещается в разделе «Документы» официального веб-сайта Учреждения reabil-nk.ru.

9. Регистрация и хранение Регламента

9.1. Настоящий Регламент регистрируется и хранится в Учреждении до замены его Регламентом в новой редакции. Копия настоящего Регламента хранится в ЛАСУ.

Подготовил
Ведущий программист Кошаров А.А.