АДМИНИСТРАЦИЯ
Ирбейского района Красноярского края

ПОСТАНОВЛЕНИЕ

05.07.2024 с. Ирбейское № 463-пг

Об утверждении Регламента парольной защиты в организациях, расположенных на территории Ирбейского района и (или) информационных системах (сетях), эксплуатируемых на территории Ирбейского района

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 12.12.2023), с частью 5 статьи 19 Федерального закона от 27 июля 2006 № 152-ФЗ «О персональных данных» (ред. от 06.02.2023), в целях предупреждения и (или) устранения последствий несанкционированного доступа к информационным ресурсам, содержащим информацию, не составляющую государственную тайну, руководствуясь статьей 38 Устава Ирбейского района, ПОСТАНОВЛЯЮ:

1. Утвердить Регламент парольной защиты в организациях, расположенных на территории Ирбейского района и (или) информационных системах (сетях), эксплуатируемых на территории Ирбейского района, согласно приложению.
2. Настоящий Регламент служит основанием при актуализации (разработке) нормативно-правовых актов по требованиям к парольной политике администраторов и пользователей ведомств (информационных систем).
3. Контроль за выполнением постановления возложить на заместителя главы района по общественно-политической работе С. А. Кузнецова.
4. Постановление вступает в силу в день, следующий за днем его официального опубликования.

Глава района О. В. Леоненко

Приложение
к постановлению администрации
Ирбейского района
от 05.07.2024 № 463-пг

РЕГЛАМЕНТ

парольной защиты в организациях, расположенных на территории Ирбейского района и (или) информационных системах (сетях), эксплуатируемых на территории Ирбейского района

1. Общие положения

1.1. Настоящий Регламент парольной защиты в ведомстве (далее - Регламент и Ведомство соответственно) разработан в целях установления общих правил, единых требований и процедур к управлению средствами аутентификации при организации парольной защиты автоматизированных рабочих мест работников ведомства и в операционных (информационных) системах (сетях) ведомства.

1.2. Регламент разработан в соответствии со следующими нормативно-правовыми актами:

Федеральным законом от 08.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 12.12.2023);

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 06.02.2023);

Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (ред. от 10.07.2023);

Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (ред. от 13.07.2015);

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» (ред. от 14.05.2020);

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» (ред. от 20.02.2020);

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).

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

1.4. Регламент устанавливает основные этапы деятельности:

по защите доступа к автоматизированным рабочим местам работников ведомства и операционным (информационным) системам (сетям) ведомства с использованием паролей;

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

по определению ответственности работников 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 операционную (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 (ИР) – 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, предназначенный для подтверждения личности или полномочий.

Системы (сети) – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления Администрации.

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 операционной (информационной) системе, утилитой генерации случайных паролей;

администратором, по правилам, заданным в операционной (информационной) системе;

самостоятельно работником ведомства при работе с операционной (информационной) системой.

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

3.4. При использовании в операционной (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 операционных (информационных) систем – 8 символов;

минимальная длина парольной фразы для пользователей с правами администратора операционных (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 – 10 попыток;

блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации на период не менее 3 минут;

максимальный срок действия пароля – не более чем 180 дней для

пользователей, не более чем 90 дней – для пользователей, обладающих повышенными полномочиями в операционных (информационных) системах. Повторное использование идентификатора пользователя исключается в течение одного года.

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

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

2.7. В случае производственной необходимости пользователю операционной (информационной) системы могут быть присвоены несколько учетных записей.

2.8. Использование несколькими работниками ведомства одного и того же имени пользователя (группового имени) запрещается.

2.9. 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 операционной (информационной) системе, автоматизированному рабочему месту является конфиденциальной информацией и должен быть известен только работнику. Работник лично несет ответственность за конфиденциальность выданного или сгенерированного им пароля.

4.2. Работник должен знать пароль доступа к автоматизированному рабочему месту и (или) операционной (информационной) системе наизусть. Запрещается хранить пароли в записанном виде на рабочем месте, в том числе на предметах мебели и деталях компьютера или иных приборов. 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 посторонними лицами.

4.5. Запрещается передача пароля другим работникам, включая непосредственных руководителей, а также работа другого работника на автоматизированном рабочем месте или в операционной (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 специалисту, ответственному за информационную безопасность/ в отдел по защите информационной безопасности ведомства. При наличии технической возможности работник должен самостоятельно в кратчайший срок изменить пароль средствами операционной (информационной) системы.

4.7. При подозрении на компрометацию пароля пользователя специалистом, ответственным за информационную безопасность/ отделом по защите информационной безопасности ведомства, осуществляется временная блокировка учетной записи и (по возможности) уведомление пользователя о необходимости изменения пароля.

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

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

5. Правила смены, прекращения и восстановления паролей

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

5.2. В операционных (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 операционной (информационной) системы.

5.3. В случае если работник забыл свой пароль доступа к операционной (информационной) системе, он обязан обратиться к администратору операционной (информационной) системы посредством личного визита или телефонной связи. В случае если сообщение о том, что пароль забыт, поступило посредством электронного письма (служебной записки), администратор операционной (информационной) системы 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 не позднее трех суток с момента получения заявки на внесение изменений.

5.7. Оператором операционной (информационной) системы локальным нормативным актом может быть введен режим блокирования учетных записей на время отпусков работников.

6. Ответственность за неисполнение настоящего Регламента

6.1. Работники ведомства 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.