КАБИНЕТ МИНИСТРОВ
РЕСПУБЛИКИ ТАТАРСТАН

ТАТАРСТАН РЕСПУБЛИКАСЫ
МИНИСТРЛАР КАБИНЕТЫ

РАСПОРЯЖЕНИЕ **БОЕРЫК**

27.04.2023 г.Казань № 972-р

В целях установления единых требований к стойкости паролей и порядка обращения с паролями на автоматизированных рабочих местах и в информационных системах, используемых в республиканских органах исполнительной власти и их подведомственных организациях:

1. Утвердить прилагаемый Регламент по организации парольной защиты в республиканских органах исполнительной власти и их подведомственных организациях.

2. Республиканским органам исполнительной власти и их подведомственным организациям, а также предложить органам местного самоуправления муниципальных образований Республики Татарстан в своей работе руководствоваться Регламентом, утвержденным настоящим распоряжением.

3. Государственному казенному учреждению «Центр цифровой трансформации Республики Татарстан» при проведении работ по созданию (модернизации) информационных систем (государственных информационных систем), которые используются в работе сотрудниками республиканских органов исполнительной власти и их подведомственных организаций, руководствоваться Регламентом, утвержденным настоящим распоряжением.

4. Контроль за исполнением настоящего распоряжения возложить на Министерство цифрового развития государственного управления, информационных технологий и связи Республики Татарстан.

Премьер-министр
Республики Татарстан А.В.Песошин

Утвержден
распоряжением
Кабинета Министров
Республики Татарстан
от 27.04. 2023 № 972-р

Регламент
по организации парольной защиты в республиканских органах исполнительной власти Республики Татарстан и их подведомственных организациях

I. Общие положения

1.1. Настоящий Регламент определяет порядок взаимодействия сотрудников республиканских органов исполнительной власти и их подведомственных организаций при организации парольной защиты на автоматизированных рабочих местах и в информационных системах, используемых в профессиональной деятельности.

1.2. Настоящий Регламент направлен на недопущение утечки персональных данных пользователей, обеспечение целостности, конфиденциальности информации, предотвращение иных информационных угроз.

1.3. Лицо, ответственное за обеспечение информационной безопасности в республиканском органе исполнительной власти, в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты, организует и контролирует функционирование системы обеспечения информационной безопасности в республиканском органе исполнительной власти, координирует функционирование систем обеспечения информационной безопасности в подведомственных организациях, в том числе соблюдение мероприятий по организации парольной защиты.

1.4. Настоящий Регламент не распространяется на правила парольной защиты автоматизированных рабочих мест, обрабатывающих сведения, составляющие государственную тайну.

1.5. Настоящий Регламент разработан в соответствии со следующими нормативными правовыми актами Российской Федерации:

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных

и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

1.6. В настоящем Регламенте используются следующие понятия:

пароль – набор символов, состоящий из букв, цифр и других символов и предназначенный для подтверждения полномочий входа сотруднику в автоматизированное рабочее место или информационную систему;

сотрудник – сотрудник республиканского органа исполнительной власти или его подведомственной организации;

учетная запись – хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к информационным системам;

информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, в том числе государственная информационная система;

компрометация пароля – факт доступа постороннего лица в автоматизированное рабочее место или в информационную систему под паролем иного сотрудника, а также подозрение на указанные действия.

II. Подготовка персонала по вопросам информационной безопасности и допуска к работе

2.1. Допуск сотрудника к работе в автоматизированном рабочем месте, а также в информационных системах осуществляется после его ознакомления с настоящим Регламентом.

2.2. Кадровая служба республиканского органа исполнительной власти или его подведомственной организации в течение трех рабочих дней со дня поступления сотрудника на государственную службу или на работу осуществляет ознакомление его с настоящим Регламентом под роспись.

III. Правила генерирования паролей

3.1. Генерирование пароля осуществляется вручную сотрудником либо автоматически с учетом следующих требований к стойкости:

минимальная длина пароля составляет:

для сотрудников – не менее 12 символов;

для сотрудников с правами администраторов – не менее 15 символов.

3.2. Пароль сотрудника содержит в себе символы не менее четырех типов (например, цифры и латинские буквы верхнего и нижнего регистров, специальные символы).

3.3. Сотруднику запрещается:

включать в пароль легко вычисляемые сочетания символов (имена, фамилии, наименования информационных систем, наименование организации, наименование отдела и т.п.), а также общепринятые сокращения и иные данные, которые можно определить, исходя из информации о пользователе (дата рождения, номер автомобиля, адрес и т.д.);

включать в пароль последовательности из более чем двух символов, расположенных рядом на клавиатуре (например, 1234asdf, qwerty678);

генерировать пароль из повторяющихся символов либо повторяющейся комбинации из нескольких символов (например, 111222ssS, psQ777psQ);

использовать пароли, заданные по умолчанию производителями оборудования (admin, user, password, administrator).

IV. Правила использования и хранения паролей

4.1. Пароль к автоматизированному рабочему месту или к информационной системе является конфиденциальной информацией и может быть известен сотруднику и администратору информационной системы. Сотрудник несет личную ответственность за конфиденциальность выданного или сгенерированного им пароля.

4.2. Запрещается передача пароля доступа другим сотрудникам, включая непосредственных руководителей, а также работа другого сотрудника в автоматизированном рабочем месте или информационной системе под паролем предыдущего пользователя, осуществившего вход в систему под своим паролем.

4.3. Набор пароля на клавиатуре должен исключать возможность наблюдения за процессом набора его другими пользователями и посторонними лицами.

4.4. При компрометации пароля сотрудник незамедлительно меняет пароль доступа средствами операционной системы (информационной системы) или обращается к администратору автоматизированного рабочего места (информационной системы) за новым паролем. О компрометации пароля сотрудник обязан немедленно сообщить непосредственному руководителю и специалисту, ответственному за информационную безопасность (при наличии).

4.5. Сотрудник обязан 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 и деталях персональной электронно-вычислительной машины. Не рекомендуется хранить пароли в мобильных телефонах, планшетах и на иных электронных носителях информации.

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

4.7. В информационной системе реализуется контроль подбора паролей. Количество неудачных попыток ввода неверного пароля, после которого доступ к информационной системе для данной учетной записи автоматически блокируется, составляет не более пяти.

V. Правила смены и прекращения действия паролей

5.1. Смена паролей доступа к автоматизированному рабочему месту и (или) информационной системе осуществляется не реже одного раза в 90 календарных дней.

5.2. Контроль срока действия пароля осуществляется автоматически, а при отсутствии технической возможности – сотрудником или администратором информационной системы.

5.3. При смене пароля выполняются следующие требования:

набор символов, из которых построен новый пароль, отличается от предыдущего не менее чем на пять символов;

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

новое значение пароля не должно совпадать с 10 предыдущими значениями паролей данного пользователя.

5.4. В автоматизированном рабочем месте и информационной системе при замене пароля реализуется автоматическая проверка пароля на соответствие минимальным требованиям стойкости, указанным в разделе IV настоящего Регламента. При отсутствии технической возможности контроль за стойкостью паролей сотрудников возлагается на администратора автоматизированного рабочего места (информационной системы).

5.5. Прекращение действия пароля при увольнении или перемещении сотрудника осуществляется удалением (отключением) его учетной записи в домене или в информационной системе, куда сотруднику ранее был предоставлен доступ. Запрещается передавать пароль перемещенного сотрудника иному сотруднику.

5.6. В случае если сотрудник забыл свой пароль доступа к информационной системе, он обязан обратиться к администратору информационной системы посредством личного визита или телефонной связи.

В случае если сообщение о том, что пароль забыт, поступило посредством электронного письма, администратор информационной системы обязан связаться с непосредственным руководителем данного сотрудника для подтверждения информации.

5.7. Восстановление пароля осуществляется путем генерирования нового пароля.
