**РАСПОРЯЖЕНИЕ**

**АДМИНИСТРАЦИИ ГЕОРГИЕВСКОГО**

**ГОРОДСКОГО ОКРУГА**

**СТАВРОПОЛЬСКОГО КРАЯ**

23 июня 2020 г. г. Георгиевск № 90-р

Об утверждении Инструкции по организации парольной защиты информационной системы персональных данных администрации Георгиевского городского округа Ставропольского края

В целях регулирования деятельности, связанной с обработкой персональных данных, осуществляемой в администрации Георгиевского городского округа Ставропольского края ее сотрудниками с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях или без использования таких средств, во исполнение требований федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», на основании статей 57, 61 Устава Георгиевского городского округа Ставропольского края

1. Утвердить прилагаемую Инструкцию по организации парольной защиты информационной системы персональных данных администрации Георгиевского городского округа Ставропольского края (далее – Инструкция).

2. Ознакомить с настоящей Инструкцией лиц, допущенных к обработке персональных данных в администрации Георгиевского городского округа Ставропольского края.

3. Руководителям структурных подразделений администрации Георгиевского городского округа Ставропольского края, обладающих правами юридического лица, руководствоваться настоящим распоряжением при организации парольной защиты информационных систем персональных данных возглавляемого структурного подразделения.

4. Признать утратившим силу пункт 6 распоряжения администрации Георгиевского городского округа Ставропольского края от 19 июня 2017 г. № 132-р «Об утверждении инструкций по обработке персональных данных в администрации Георгиевского городского округа Ставропольского края».

5. Контроль за выполнением настоящего распоряжения возложить на заместителя главы администрации – начальника управления по общественной безопасности администрации Георгиевского городского округа Ставропольского края Бережного Г.А.

6. Настоящее распоряжение вступает в силу со дня его принятия.

Исполняющая полномочия Главы

Георгиевского городского округа

Ставропольского края Ж.А.Донец

УТВЕРЖДЕНА

распоряжением администрации

Георгиевского городского

округа Ставропольского края

от 23 июня 2020 г. № 90-р

ИНСТРУКЦИЯ

по организации парольной защиты информационной системы

персональных данных администрации Георгиевского городского округа Ставропольского края

1. Общие сведения

Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в администрации Георгиевского городского округа Ставропольского края (далее – администрация), а также контроль за действиями пользователей и обслуживающего персонала систем при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на ответственных за техническое обеспечение работы систем и средств автоматизации в администрации.

2. Требования к паролям

2.1. Личные пароли доступа к элементам информационной системы персональных данных создаются пользователем самостоятельно, за исключением временного пароля, который выдает ответственный за техническое обеспечение работы систем и средств автоматизации в администрации.

2.2. Пользователь обязан сменить временный пароль, выданный ответственным за техническое обеспечение работы систем и средств автоматизации в администрации при первом входе в систему.

2.3. Правила формирования пароля:

пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

длина пароля должна быть не менее 8 символов;

в пароле должны присутствовать символы трех категорий из числа следующих четырех:

прописные буквы английского алфавита от A до Z;

строчные буквы английского алфавита от a до z;

десятичные цифры от 0 до 9;

символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования персональных компьютеров и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

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

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

запрещается выбирать пароли, которые уже использовались ранее;

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

личный пароль пользователь не имеет права сообщать никому.

2.4. Владельцы паролей должны быть ознакомлены под подпись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

2.5. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система генерации паролей должна исключать возможность ознакомления других сотрудников с паролями исполнителей.

2.6. Правила ввода пароля:

ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3. Смена паролей

3.1. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в два месяца.

3.2. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри администрации и т.п.) должна производиться ответственными за техническое обеспечение работы систем и средств автоматизации в администрации немедленно после окончания последнего сеанса работы данного пользователя с системой.

3.3. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри администрации и другие обстоятельства) ответственных за техническое обеспечение работы систем и средств автоматизации в администрации и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем сегмента.

4. Хранение и контроль

4.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

4.2. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

4.3. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность или у руководителя подразделения в опечатанном личной печатью пенале.

4.4. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей структурных подразделений администрации, периодический контроль – возлагается на администраторов средств парольной защиты.

4.5. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры по изменению пароля и выявлению последствий компрометации.

4.6. Лица, использующие паролирование, обязаны:

четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

своевременно сообщать ответственным за техническое обеспечение работы систем и средств автоматизации в администрации об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_