**РАСПОРЯЖЕНИЕ**

**АДМИНИСТРАЦИИ ГЕОРГИЕВСКОГО**

**ГОРОДСКОГО ОКРУГА**

**СТАВРОПОЛЬСКОГО КРАЯ**

23 июня 2020 г. г. Георгиевск № 92-р

Об утверждении Инструкции пользователя 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 пользователя информационной системы персональных данных в 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.

4. Признать утратившим силу пункт 1 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. № 92-р

ИНСТРУКЦИЯ

пользователя информационной системы персональных данных в

администрации Георгиевского городского округа Ставропольского края

1. Общие сведения

1.1. Настоящая Инструкция определяет общие права и обязанности сотрудников, допущенных к обработке персональных данных на средствах вычислительной техники сегмента администрации Георгиевского городского округа Ставропольского края (далее – администрация округа).

1.2. Настоящая Инструкция предназначена для руководителей структурных подразделений и пользователей, осуществляющих обработку информации, содержащей персональные данные.

1.3. Пользователем является каждый работник администрации округа, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.4. Пользователь в своей работе руководствуется документами по защите информации Федеральной службы по техническому и экспортному контролю России, внутренними документами администрации округа, настоящей Инструкцией.

2. Общие права и обязанности пользователей при работе

в информационной системе персональных данных

2.1. Каждый сотрудник администрации округа, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным, несет персональную ответственность за свои действия и имеет право доступа в соответствии с матрицей доступа, а также обязан:

2.1.1.Знать и выполнять требования настоящей Инструкции и других нормативных правовых документов администрации округа по защите персональных данных. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами сегмента.

2.1.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в администрации округа.

2.1.3. Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.1.4. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.

2.1.5. Соблюдать правила при работе в информационно-телекоммуникационной сети «Интернет» (раздел 3 настоящей инструкции).

2.1.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нём информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.1.7. Хранить в тайне свои пароли, выполнять требования Инструкции по организации парольной защиты.

2.1.8. Передавать для хранения в установленном порядке свои реквизиты разграничения доступа только руководителю своего подразделения или ответственному за обработку персональных данных в подразделении (в пенале, опечатанном своей личной печатью).

2.1.9. Надежно хранить и никому не передавать личную печать, используемую для опечатывания пенала с личными реквизитами доступа при передаче его на хранение ответственному за обработку персональных данных или руководителю подразделения.

2.1.10. Выполнять требования инструкции по организации антивирусной защиты в части, касающейся действий пользователей.

2.1.11. Немедленно уведомлять ответственного за обработку персональных данных в подразделении и ставить в известность руководителя подразделения в случае утери личных реквизитов доступа или при подозрении компрометации личных паролей, а также при обнаружении:

1) нарушений целостности пломб (наклеек) на аппаратных средствах сегмента или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее – НСД) к техническим средствам сегмента;

2) несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств сегмента;

3) отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию информационной системы персональных данных, выхода из строя или неустойчивого функционирования узлов персонального компьютера или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

4) некорректного функционирования установленных в сегменте технических средств защиты;

5) непредусмотренных техническим паспортом сегментаотводов кабелей и подключенных устройств.

2.1.12. При отсутствии визуального контроля за рабочей станцией, доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl>, <Alt>, <Del> и выбрать опцию <Блокировка>.

2.1.13. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий в рамках возложенных на него функций.

2.1.14. Присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним персонального компьютера в подразделении.

2.1.15. Контролировать вывод информации на съемные носители информации. Гриф на носителе должен быть не ниже грифа записываемой информации.

2.2. Пользователям категорически запрещается:

2.2.1. Использовать компоненты программного и аппаратного обеспечения информационной системы персональных данных в неслужебных целях.

2.2.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств информационной системы персональных данных или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные техническим паспортом системы.

2.2.3. Осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.

2.2.4. Записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (гибких магнитных дисках и т.п.).

2.2.5. Копировать защищаемую информацию на внешние носители без письменного разрешения руководителя структурного подразделения.

2.2.6. Оставлять включенным без присмотра персональный компьютер, не активизировав средства защиты от НСД.

2.2.7. Оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения).

2.2.8. Использовать в сегменте неучтенные съемные носители информации.

2.2.9. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок ставить в известность ответственных за техническое обеспечение работы систем и средств автоматизации в администрации и руководителя своего подразделения.

2.2.10. Разглашать защищаемую информацию третьим лицам.

2.2.11. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

2.2.12. Не санкционировано открывать общий доступ к ресурсам.

2.2.13. Подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства.

2.2.14. Отключать (блокировать) средства защиты информации.

2.2.15. Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационной системе персональных данных.

2.2.16. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системы персональных данных.

2.2.17. Привлекать посторонних лиц для выполнения ремонта или настройки АРМ без согласования с ответственными за техническое обеспечение работы систем и средств автоматизации в администрации.

2.3. Действия пользователей до идентификации и аутентификации в системе

2.3.1. Пользователям разрешается:

производить включение, выключение, перезагрузку технических средств;

предъявлять личный идентификатор и вводить пароль для авторизации в системе.

Пользователям запрещается:

входить в настройки базовой системы ввода-вывода технических средств и систем персонального компьютера;

осуществлять загрузку нештатных операционных систем со сторонних носителей информации.

3. Правила работы в информационно-телекоммуникационной

сети «Интернет»

3.1. Работа в информационно-телекоммуникационной сети «Интернет» (далее – Сеть) на элементах информационной системы персональных данных должна проводиться при служебной необходимости.

3.2. При работе в Сети запрещается:

3.2.1. Осуществлять работу при отключенных средствах защиты (антивирусных и других).

3.2.2. Передавать по Сети защищаемую информацию без использования средств шифрования.

3.2.3. Запрещается скачивать из Сети программное обеспечение и исполняемые файлы (файлы с расширением exe, dll, msi).

3.2.4. Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое программное обеспечение и другие).

3.2.5. Запрещается нецелевое использование подключения к Сети.

4. Ответственность

Сотрудники администрации округа, нарушившие требования данной инструкции, несут ответственность в соответствии с действующим законодательством Российской Федерации.

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