ПРИЛОЖЕНИЕ № 2

к постановлению администрации

муниципального образования

город Краснодар

от 25.09.2020 № 4144

**ПРАВИЛА**

**доступа в помещения администрации муниципального**

**образования город Краснодар, в которых ведётся**

**обработка персональных данных с использованием средств**

**автоматизации в рабочее, нерабочее время**

**и в нештатных ситуациях**

**Раздел I**

**Общие положения**

1. Настоящие Правила доступа в помещения администрации муниципального образования город Краснодар, в которых ведётся обработка персональных данных с использованием средств автоматизации в рабочее, нерабочее время и в нештатных ситуациях (далее – Правила), устанавливают организационные основы доступа в помещения администрации муниципального образования город Краснодар, в которых размещены отраслевые, функциональные и территориальные органы администрации муниципального образования город Краснодар (далее – органы администрации), в которых ведётся обработка персональных данных с использованием средств автоматизации. Правила разработаны в целях обеспечения безопасности информации, обрабатываемой в органах администрации, на средствах вычислительной техники информационных систем, на съёмных носителях информации, а также для обеспечения внутриобъектового режима.
2. Настоящие Правила распространяются на доступ в следующие помещения органов администрации:

помещения, в которых происходит обработка персональных данных с использованием средств автоматизации, в том числе серверные помещения;

помещения, в которых хранятся материальные, в том числе съёмные элетронные носители персональных данных и их резервные копии.

1. Настоящие Правила разработаны в соответствии с:

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

постановлением Правительства Российской Федерации от 21.03.2012 № 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»;

приказом Федеральной службы безопасности России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости»;

приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

1. Работники органов администрации, допущенные в помещения,   
   в которых происходит обработка персональных данных с использованием средств автоматизации, а также в которых хранятся материальные, в том числе съёмные электронные носители персональных данных и их резервные копии (далее – Помещения), обязаны:

выполнять требования обеспечения безопасности персональных данных;

соблюдать режим конфиденциальности при обращении с персональными данными, носителями персональных данных;

своевременно выявлять попытки посторонних лиц получить сведения о персональных данных.

**Раздел II**

**Общие требования к оборудованию помещений**

**и регламентации доступа в них в рабочее, нерабочее время**

**и нештатных ситуациях**

1. Режим обеспечения безопасности Помещений должен быть организован таким образом, чтобы препятствовать возможности неконтролируемого проникновения или пребывания в этих Помещениях лиц, не имеющих права доступа в эти Помещения.
2. Помещения оснащаются надёжными входными дверьми с замками в случае отсутствия контроля периметра или системы видеонаблюдения, или системы контроля и управления доступом в Помещение.
3. В случае отсутствия контроля периметра или системы видеонаблюде­ния или системы контроля и управления доступом окна Помещения, расположенного на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц, должны быть оборудованы металлическими решётками или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в Помещения.
4. В органах администрации определяется перечень помещений, в которых происходит обработка персональных данных. Форма перечня приведена в приложении № 1 к настоящим Правилам.
5. Доступ работников в Помещения органов администрации должен быть организован согласно перечню лиц, допущенных в Помещения обработки персональных данных (форма перечня приведена в приложении № 2 к настоящим Правилам). Перечень работников, доступ которых разрешён в Помещения, утверждается руководителем органа администрации и размещается на внутренней стороне двери этого Помещения.
6. В Помещениях определяются места хранения материальных (в том числе съёмных) носителей персональных данных и лиц, ответственных за их сохранность (форма перечня мест хранения материальных носителей персональных данных приведена в приложении № 3 к настоящим Правилам).
7. Работа с персональными данными выполняется только в пределах контролируемой зоны, то есть в пределах помещений, занимаемых органами администрации, в которых исключено неконтролируемое пребывание посторонних лиц. При работе с информацией на бумажном носителе, содержащей персональные данные, исполнитель должен иметь на рабочем столе только те документы, которые находятся на исполнении. При выходе из кабинета всех работников кабинет закрывается на замок.
8. Доступ посторонних лиц в Помещения должен осуществляться только ввиду служебной необходимости и в присутствии работника, допущенного в Помещение. При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с персональными данными.
9. В нерабочее время все окна и двери в Помещениях (в том числе в смежные Помещения), в которых ведётся обработка персональных данных, должны быть надёжно закрыты, материальные (в том числе съёмные) носители должны быть убраны в надёжные хранилища, компьютеры выключены либо заблокированы.
10. При необходимости повышенного уровня обеспечения безопасности Помещений могут использоваться системы видеонаблюдения и системы контроля и управления доступом.
11. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в Помещения в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации может осуществляться без сопровождающих лиц.

**Раздел III**

**Особенности доступа в серверные Помещения в рабочее,**

**нерабочее время и нештатных ситуациях**

1. Доступ в серверные Помещения посторонних лиц осуществляется на основании служебной записки, направленной в адрес руководителя органа администрации, ответственного за данное серверное Помещение.
2. Двери серверных Помещений должны быть оборудованы устройствами, обеспечивающими постоянное закрытие дверей на замок и их открытие только для санкционированного прохода.
3. Уборка серверных Помещений происходит только под контролем сопровождающего лица из числа работников, допущенных в Помещения.
4. Нахождение в серверных Помещениях посторонних лиц без сопровождающего лица, допущенного в серверное Помещение, запрещено.
5. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные Помещения в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации может осуществляться без согласования с ответственным за доступ в Помещения.
6. Сотрудники органов Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий и аварийных служб, врачи «скорой помощи» допускаются в серверные помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении работника, допущенного к работе в Помещении.

Исполняющий обязанности

начальника управления

информационно-коммуникационных

технологий и связи администрации

муниципального образования

город Краснодар В.В.Лысенко