



БЕЛГОРОДСКАЯ ОБЛАСТЬ

**АДМИНИСТРАЦИЯ НОВООСКОЛЬСКОГО
ГОРОДСКОГО ОКРУГА**

РАСПОРЯЖЕНИЕ

Новый Оскол

«20» ноября 2020г.

№ 1328-п

**Об утверждении Порядка доступа
в помещения, в которых ведется
обработка персональных данных**

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 года № 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 в целях совершенствования работы по обеспечению защиты персональных данных в администрации Новооскольского городского округа:

1. Утвердить Порядок доступа в помещения, в которых ведется обработка персональных данных (далее – Порядок) (прилагается).

2. Лицам, исполняющим должностные обязанности, предусматривающие осуществление обработки персональных данных либо осуществление доступа к персональным данным руководствоваться положениями Порядка, утвержденного пунктом 1 данного распоряжения.

3. Начальнику информационно-аналитического отдела администрации Новооскольского городского округа (Мурашко Н.Н.) обеспечить размещение настоящего распоряжения на официальном сайте органов местного самоуправления Новооскольского городского округа Белгородской области в информационно-телекоммуникационной сети общего пользования.

4. Контроль за исполнением распоряжения возложить на заместителя главы администрации Новооскольского городского округа – руководителя аппарата главы администрации Новооскольского городского округа Прокущенко Л.Д.

**Глава администрации
Новооскольского городского округа**

А.Н. Гриднев

Утвержден
распоряжением администрации
Новооскольского городского округа
от «20» ноября 2020 года № 1328-п

**Порядок
доступа в помещения, в которых ведется обработка
персональных данных**

1. Общие положения

1.1. Настоящий порядок доступа в помещения, в которых ведется обработка персональных данных (далее – Порядок) разработан в целях выполнения требований Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21, постановления Правительства РФ от 21 марта 2012 года № 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» в администрации Новооскольского городского округа (далее – Учреждение).

1.2. Также, Порядок регламентирует доступ в помещения, в которых расположены элементы информационных систем персональных данных, в рабочее и нерабочее время, а также в нестандартных ситуациях в соответствии с приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении Составы 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 защищенности».

1.3. Настоящий Порядок разработан в целях обеспечения безопасности персональных данных при их обработке (в том числе хранении) путем создания условий, затрудняющих несанкционированный доступ к техническим средствам, участвующим в обработке персональных данных, и материальным носителям персональных данных.

1.4. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации,

а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

Данный режим обеспечивается:

- оснащением помещения охранной и пожарной сигнализацией;
- обязательным запираением помещения на ключ, даже при выходе из него в рабочее время;
- отдельным хранением дубликатов ключей;
- закрытием металлических шкафов и сейфов, где хранятся носители информации, содержащие персональные данные.

1.5. Настоящий Порядок должен соблюдаться всеми сотрудниками Учреждения.

2. Доступ в помещения в рабочее время

2.1. В рабочее время доступ в помещения, в которых расположены элементы информационной системы персональных данных (далее – ИСПДн) Учреждения, разрешен только работникам Учреждения, указанным в соответствующем перечне лиц.

2.2. В рабочее время помещения, где расположены элементы ИСПДн, должны закрываться на замок и открываться только для санкционированного прохода.

2.3. Доступ обслуживающего персонала для уборки помещения допускается только в присутствии пользователей ИСПДн.

3. Доступ в помещения в нерабочее время

3.1. В нерабочее время доступ в помещения, в которых расположены элементы ИСПДн Учреждения, разрешен только работникам Учреждения, указанным в соответствующем перечне лиц при наличии служебной записки, подписанной руководителем подразделения и заверенной ответственным за обеспечение безопасности персональных данных с занесением записи в «Журнал доступа в помещения, где расположены элементы ИСПДн, в нерабочее время».

4. Доступ в помещения в нестандартных ситуациях

4.1. Если перед вскрытием помещений обнаружено нарушение целостности замков, то помещения не вскрываются, составляется акт о случившемся и немедленно докладывается руководителю организации, ответственному за обеспечение безопасности персональных данных, и принимаются меры по охране помещений до прибытия службы безопасности.

4.2. В дневное время суток сотрудник, обнаруживший нештатную ситуацию, должен поставить в известность непосредственного руководителя структурного подразделения – устно, ответственного за обеспечение безопасности персональных данных – устно, при необходимости – письменно.

4.3. В ночное время суток при возникновении нештатной ситуации, должна быть оповещена служба безопасности (охрана). Событие в обязательном порядке регистрируется в журнале дежурств, с указанием точного времени инцидента, краткого описания событий, с указанием Ф.И.О. оповещенных лиц, описанием действий, направленных на устранение нештатной ситуации. Если создается угроза уничтожения персональных данных, то дежурный имеет право вскрыть помещения и принять меры к спасению технических средств и документов. При этом также составляется рапорт о случившемся и немедленно докладывается лицу, ответственному за обеспечение безопасности персональных данных.



Приложение 1
к Порядку доступа в помещения, в
которых ведется обработка
персональных данных

Типовая форма журнала доступа в помещения, где расположены элементы ИСПДн,
в нерабочее время

№ п/п	Дата и время	Ф.И.О.	Помещение	Подпись сотрудника	Время приема под охрану	Подпись работника охраны
1	2	3	4	5	6	7

