****

**АДМИНИСТРАЦИЯ**

**БОЛЬШЕСОЛДАТСКОГО РАЙОНА КУРСКОЙ ОБЛАСТИ**

РАСПОРЯЖЕНИЕ

от 15.09.2022 № 210-р

с. Большое Солдатское

**Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных**

В соответствии с [Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»](http://docs.cntd.ru/document/901990046), с целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Администрации Большесолдатского района Курской области и подведомственных ей учреждениях:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Администрации Большесолдатского района Курской области и подведомственных ей учреждениях, согласно приложению к настоящему распоряжению.

2. Главному специалисту–эксперту по обеспечению предоставления муниципальных услуг, вопросам обращений граждан Администрации Большесолдатского района Курской области Божедомовой Полине Григорьевне обеспечить опубликование настоящего распоряжения на официальном сайте Администрации Большесолдатского района Курской области в информационно-телекоммуникационной сети «Интернет».

3. Контроль за исполнением распоряжения возложить на исполняющую обязанности Управляющего делами Администрации Большесолдатского района Курской области Боровлеву Любовь Васильевну.

4. Распоряжение вступает в силу со дня его официального опубликования.

Глава

Большесолдатского района

Курской области В.Зайцев

Приложение

к распоряжению Администрации

Большесолдатского района

Курской области

от 15.09.2022 № 210-р

**УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ,**

**актуальные при обработке персональных данных в информационных системах персональных данных**

**1. Общие положения**

1.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Администрации Большесолдатского района Курской области и подведомственных ей учреждениях (далее - ОМСУ и учреждения), разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.2. При разработке угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных (далее - ИСПДн) использованы правовые акты:

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

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

3) Указ Президента Российской Федерации от 17 марта 2008 года №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

4) Указ Президента Российской Федерации от 22 мая 2015 года №260 «О некоторых вопросах информационной безопасности Российской Федерации»;

5) Постановление Правительства Российской Федерации от 1 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

6) Приказ Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России) от 18 февраля 2013 года N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее - Приказ ФСТЭК России);

7) Приказ Федеральной службы безопасности Российской Федерации (далее - ФСБ России) от 10 июля 2014 года N 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 защищенности» (далее - Приказ ФСБ России);

8) Приказ ФСБ России от 9 февраля 2005 года N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

9) Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра [ФСБ России от 31 марта 2015 года N 149/7/2/6-432](http://docs.cntd.ru/document/420336137) (далее - Методические рекомендации ФСБ России по разработке НПА);

10) Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России от 14 февраля 2008 года;

11) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России от 15 февраля 2008 года (далее - Базовая модель угроз).

1.3. Угрозы безопасности персональных данных, актуальные при обработке персональных данных, уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн.

1.4. ИСПДн ОМСУ и учреждений имеют сходную структуру, однотипны и характеризуются тем, что в качестве объектов информатизации выступают распределенные информационные системы, имеющие, как правило, одноточечное подключение к сетям общего пользования. В зависимости от конкретного объекта информатизации ИСПДн могут охватывать многие подразделения ОМСУ и быть развернуты в пределах нескольких близко расположенных зданий. В отдельных случаях используется локальная ИСПДн, развернутая в пределах одного здания.

1.5. ИСПДн ОМСУ и учреждений представляют собой совокупность изолированных друг от друга информационных систем.

1.6. Ввод персональных данных в ИСПДн и вывод данных из ИСПДн осуществляется с использованием бумажных и электронных носителей информации. В качестве электронных носителей информации используются учтенные съемные носители информации и оптические диски. Доступ к ИСПДн ограничен перечнем муниципальных служащих ОМСУ либо субъектами персональных данных.

1.7. В отдельных случаях при обработке персональных данных в ИСПДн могут применяться технологии виртуализации.

1.8. Персональные данные субъектов персональных данных обрабатываются с целью получения муниципальных услуг, а также:

в целях обеспечения деятельности структурных подразделений ОМСУ и учреждений;  
в целях обеспечения кадровой работы, в том числе в целях содействия муниципальным служащим в прохождении муниципальной службы, выполнении работы, в обучении и должностном росте, обеспечения личной безопасности муниципальных служащих и членов их семей, обеспечения сохранности принадлежащего им имущества и имущества ОМСУ и учреждений, учета результатов исполнения ими должностных обязанностей, обеспечения установленных законодательством Российской Федерации условий осуществления служебной деятельности и труда, гарантий и компенсаций;

в целях формирования кадрового резерва на муниципальной службе, резерва управленческих кадров ОМСУ, противодействия коррупции;

в целях реализации процедур по представлению граждан к награждению;

в целях приема, обработки и распределения поступивших в адрес ОМСУ, Главы Большесолдатского района Курской области документов, обращений граждан и организаций, а также регистрации и отправки исходящей корреспонденции;

в целях ведения внутренней служебной переписки;

в целях формирования внутренних документов, регламентирующих деятельность ОМСУ и учреждений;

в целях взаимодействия со средствами массовой информации.

1.9. Оператором персональных данных при их обработке в ИСПДн ОМСУ и учреждений является ОМСУ и учреждения, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных. Непосредственную обработку персональных данных в ИСПДн осуществляют уполномоченные соответствующим ОМСУ и учреждением структурные подразделения (сотрудники).

1.10. Информационный обмен по сетям связи общего пользования осуществляется с использованием сертифицированных средств криптографической защиты информации (далее - СКЗИ).

1.11. Контролируемой зоной ИСПДн являются административное здание ОМСУ и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей, серверы, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования.

1.12. Технические средства и базы данных ИСПДн ОМСУ и учреждений размещаются на территории Российской Федерации.

**2. Характеристики безопасности информационных систем персональных данных**

2.1. Учитывая особенности обработки персональных данных в ОМСУ и учреждениях, а также категорию и объем обрабатываемых в ИСПДн персональных данных, основными характеристиками информационной безопасности ИСПДн являются конфиденциальность, целостность и доступность.

В целях настоящего нормативного правового акта используются следующие понятия основных характеристик информационной безопасности ИСПДн:

конфиденциальность - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

целостность - состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения;

доступность - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

2.2. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные неправомерные действия с персональными данными.

2.3. В зависимости от состава обрабатываемых персональных данных и типа актуальных угроз необходимый уровень защищенности персональных данных для каждой ИСПДн определяется индивидуально.

2.4. Угрозы безопасности персональных данных, обрабатываемых в информационных системах персональных данных, приведенные в Актуальных угрозах безопасности ИСПДн, подлежат адаптации в ходе разработки частных моделей угроз безопасности персональных данных.

**3. Применение средств криптографической защиты информации в информационных системах персональных данных**

3.1. Актуальность применения в ИСПДн ОМСУ и учреждений СКЗИ определяется необходимостью защиты персональных данных, в том числе при информационном обмене по сетям связи общего пользования.

3.2. СКЗИ предназначены для защиты информации от действий со стороны лиц, не имеющих право доступа к этой информации.

3.3. Принятыми организационно-техническими мерами в ОМСУ и учреждениях исключена возможность несанкционированного доступа потенциального нарушителя к ключевой информации СКЗИ.

3.4. При эксплуатации СКЗИ соблюдаются требования эксплуатационно-технической документации на СКЗИ и требования действующих нормативных правовых актов в области реализации и эксплуатации СКЗИ.

3.5. Для обеспечения безопасности персональных данных при их обработке в ИСПДн используются СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия.

3.6. Объектами защиты в ИСПДн являются:

персональные данные;

средства криптографической защиты информации;

среда функционирования СКЗИ;

информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

документы, дела, журналы, картотеки, издания, технические документы, видео, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты среды функционирования СКЗИ;

носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

используемые информационной системой каналы (линии) связи, включая кабельные системы;

помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

**4. Определение возможностей создания способов, подготовки и проведения атак на объекты защиты**

4.1. Реализация угроз безопасности персональных данных, обрабатываемых в ИСПДн, определяется возможностями источников атак:

- возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны;

- возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы СКЗИ и среда их функционирования;

- возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования;

- возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ);

- возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения);

- возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ).

4.2. Актуальными признаны:

- возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны;

- возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к АС, на которых реализованы СКЗИ и среда их функционирования.