

**АДМИНИСТРАЦИЯ**

**муниципального района «Мещовский район»**

Калужской области

**ПОСТАНОВЛЕНИЕ**

16 мая 2017г. № 319

**Об утверждении порядка выполнению требований по обеспечению безопасности персональных данных в информационных системах персональных данных Администрации муниципального района «Мещовский район», эксплуатируемых с использованием криптосредств**

На основании ст. ст. 15,43 Федерального закона от 6 октября 2003 г. №131 "Об общих принципах организации местного самоуправления в Российской Федерации", Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСБ РФ 21 февраля 2008 г. № 149/6/6-622), администрация муниципального района «Мещовский район»

**ПОСТАНОВЛЯЕТ:**

1. Утвердить Порядок выполнению требований по обеспечению безопасности персональных данных в информационных системах персональных данных Администрации муниципального района «Мещовский район», эксплуатируемых с использованием криптосредств (прилагается)

3. Настоящее постановление вступает в силу с момента подписания.

**Глава администрации В.Г. Поляков**

Приложение №1

к Постановлению Администрации

муниципального района «Мещовский район»

от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2017 г. № \_\_\_\_\_\_\_\_

**Порядок выполнению требований по обеспечению безопасности персональных данных в информационных системах персональных данных Администрации муниципального района «Мещовский район», эксплуатируемых с использованием криптосредств**

В целях выполнения требований Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСБ РФ 21 февраля 2008 г. № 149/6/6-622) принять следующие организационные и технические меры:

1. Организация системы защиты персональных данных
   1. В Администрации муниципального района «Мещовский район» (далее - Администрация, Оператор) должен быть назначен ответственный за обеспечение безопасности персональных данных (далее - ПДн) в информационных системах персональных данных (далее - ИСПДн).
   2. Администрацией должны быть разработаны и введены в действие документы, регламентирующие работу с ПДн.
   3. Необходимо вести учет пользователей, допущенных к работе в ИСПДн.
   4. В соответствии с п.1 постановления 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» необходимо определить перечень должностей, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн.
   5. В соответствии с п.5 ч.2 ст.19 Федерального закона «О персональных данных» необходимо вести учет машинных носителей ПДн. Форма Журнала учета отчуждаемых машинных носителей персональных данных утверждена нормативным актом Администрации.
   6. Необходимо обеспечить сохранность носителей ПДн, которые предназначены для передачи ПДн в рамках договоров, заключенных между Администрацией и третьими лицами.
   7. В соответствии с п.1 указа Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» при необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном [законодательством](garantF1://10002673.28) Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.
2. Организация системы криптографических мер защиты информации
   1. На используемые ИСПДн должны быть разработаны модели угроз безопасности ПДн.
   2. В соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» необходимо установить уровень защищенности ПДн при их обработке в ИСПДн.
3. Разрешительная и эксплуатационная документация
   1. Необходимо иметь акты ввода в эксплуатацию криптосредств.
   2. В имеющихся формулярах на криптосредства должны присутствовать записи о закреплении изделия при эксплуатации.
4. Требования к обслуживающему персоналу
   1. Администрацией должен быть назначен ответственный пользователь криптосредств.
   2. Ответственному пользователю криптосредств необходимо ознакомиться с Инструкцией ответственного пользователя криптосредств под роспись.
   3. Ответственному пользователю криптосредств необходимо провести обучение по работе с криптосредствами.
   4. В должностные инструкции ответственного пользователя криптосредств должны быть внесены необходимые коррективы, связанные с исполнением служебных обязанностей по данному направлению, в соответствии с Рекомендациями по внесению изменений в должностные инструкции персонала в части обеспечения безопасности ПДн при их обработке в ИСПДн.
   5. Необходимо вести учет лиц, допущенных к работе с криптосредствами. Перечень сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных (пользователи криптосредств), утвержден нормативным актом Администрации.
   6. Пользователям криптосредств необходимо ознакомиться с Инструкцией пользователя криптосредств под роспись.
5. Эксплуатация криптосредств
   1. Необходимо вести журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов (далее - Журнал). Форма соответствующего Журнала утверждена нормативным актом Администрации. Правила заполнения Журнала представлены в Приложении № 1 к настоящим Рекомендациям.
6. Организационные меры
   1. При размещении криптосредств должны соблюдаться условия, указанные в ч.4 типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСБ РФ 21 февраля 2008 г. № 149/6/6-622).

ПРИЛОЖЕНИЕ № 1

к Рекомендациям по выполнению требований по обеспечению безопасности персональных данных в информационных системах персональных данных Администрации муниципального района «Мещовский район», эксплуатируемых с использованием криптосредств

**Правила заполнения журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов**

1. В поле «Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов» необходимо вписать название СКЗИ;
2. В поле «**Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов**» необходимо вписать данные из формуляра (формуляр выдается производителем вместе с криптосредством);
3. В поле «**Номера экземпляров (криптографические номера) ключевых документов**» необходимо вписать номер (заводской/инвентарный) носителя ключевой информации (сертификатов электронных подписей и т.д.);
4. В поле «**Отметка о получении**» пишется название организации-поставщика криптосредства и дата получения;
5. В поле «**Отметка о выдаче**» пишется ФИО пользователя СКЗИ в организации, дата, подпись;
6. В поле «**Отметка о подключении (установке) СКЗИ**» необходимо вписать данные из акта установки СКЗИ: ФИО сотрудника органа криптографической защиты, произведшего установку, дата, номер аппаратного средства – это номер компьютера, на котором установлено СКЗИ;
7. Поле «Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов» заполняется только в случае изъятия, уничтожения СКЗИ.