МУНИЦИПАЛЬНОЕ КАЗЁННОЕ УЧРЕЖДЕНИЕ АНЖЕРО-СУДЖЕНСКОГО ГОРОДСКОГО ОКРУГА «ФУНКЦИОНАЛЬНО-АНАЛИТИЧЕСКИЙ ЦЕНТР»

ПРИКАЗ

от 23.08.2018г. **№73**

Об утверждении порядка обеспечения безопасности ПДн при помощи криптосредств

Руководствуясь требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных", Постановления Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Постановления Правительства Российской Федерации от 21.03.2012 N 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 защиты персональных данных граждан, обрабатываемых в муниципальном казённом учреждении Анжеро-Судженского городского округа «Функционально-аналитический центр»,

ПРИКАЗЫВАЮ:

1.Утвердить прилагаемый Порядок обеспечения безопасности ПДн при помощи криптосредств в муниципальном казённом учреждении Анжеро-Судженского городского округа «Функционально-аналитический центр» (далее - Положение).

2.Главному специалисту отдела информационной и кадровой работы МКУ «ФАЦ» Белоусовой А.С. ознакомить Белоногова А.С., главного специалиста МБУ «ЦБ УО» с настоящим руководством и обеспечить его исполнение.

3.Контроль за исполнением приказа возложить на начальника юридического отдела МКУ «ФАЦ» Модель А.В

Директор МКУ «ФАЦ» С.А. Вейс

С приказом ознакомлены

Утверждено
приказом МКУ «ФАЦ»
от 23.08.2018г. № 73

Порядок
обеспечения безопасности персональных данных при помощи криптосредств

1. Основные термины и определения

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Доступ к информации - возможность получения информации и ее использования.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Контролируемая зона - пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.
Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

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

Криптосредство - шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц, которым предоставлен с согласия субъекта персональных данных или на которые, в соответствии с федеральными законами, не распространяется требование соблюдения конфиденциальности.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами

организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные (ПДн)- любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь - лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Режимные помещения - помещения, где установлены криптосредства или хранятся ключевые документы к ним.

Средство защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Шифровальные (криптографические) средства - криптосредства:

а) средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

б) средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной цифровой подписи - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

г) средства кодирования - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);
е) ключевые документы (независимо от вида носителя ключевой информации).

2. Общие положения

2.1. Настоящие Требования разработаны на основании требований Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ "О персональных данных", Типовых требований ФСБ от 21.02.2008 № 149/6/6-622
2.2. Настоящие требования определяют порядок организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в муниципальном казённом учреждении Анжеро –Судженского городского округа «Функционально-аналитический центр» (далее – ИСПДн) в (далее – Оператор).

3. Организация и обеспечение безопасности обработки с использованием шифровальных (криптографических) средств персональных данных

3.1. Криптографические средства должны быть установлены и введены в эксплуатацию в соответствии с эксплуатационной и технической документацией к этим средствам.
3.2. Перед непосредственной эксплуатацией криптосредства проходят проверку готовности с составлением заключений о возможности их эксплуатации.
3.3. Список лиц (пользователей), допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах, оформляется документально. Перечисленные должностные лица должны пройти обучение по работе с криптосредствами.
3.4. Пользователи криптосредств обязаны:

- Не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты.
- Соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним.
- Сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним.
- Немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.
- Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным

настоящими Требованиями, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

3.5. Оператором назначается ответственный за эксплуатацию криптосредств из числа штатных сотрудников, который осуществляет контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним.

3.6. Ответственный обязан контролировать:

- Соблюдение пользователями криптосредств конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документах к ним.
- Точное выполнение пользователями криптосредств требований к обеспечению безопасности персональных данных.
- Надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения.
- Своевременное выявление попыток посторонних лиц получить сведения о защищаемых персональных данных, об используемых криптосредствах или ключевых документах к ним.
- Немедленное принятие мер по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

3.7. Криптосредства, эксплуатационная и техническая документация подлежат поэкземплярному учету.

3.8. Передача по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

4. Условия размещения и охраны помещений, в которых установлены криптографические средства

4.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее – режимные помещения), должны обеспечивать сохранность персональных данных, криптосредств и ключевых документов к ним.

4.2. Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

4.3. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.
4.4. Режимные помещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.
4.5. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе ответственного пользователя криптосредств. Дубликат ключа от хранилища ответственного пользователя криптосредств в опечатанной упаковке должен быть передан на хранение оператору под расписку в соответствующем журнале.
4.6. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале ответственному пользователю криптосредств или уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.
4.7. В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств, ответственным пользователем криптосредств или оператором.

Лист ознакомления с инструкцией

№ п/п	Ф.И.О. работника	Должность работника	Дата ознакомления с инструкцией и получения копии инструкции	Личная подпись
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				