**Требования к выполнению обязанностей операторов персональных данных по организации обработки персональных данных, и обеспечению безопасности информации на автоматизированных рабочих местах государственной информационной системы Ленинградской области «Контингент-ЛО»**

Для выполнения основных мероприятий необходимо:

1) установить и настроить следующие программные средства защиты информации, сертифицированные по требованиям безопасности информации:

- ViPNet Client 3.х (КС3) **для подключения к защищенной сети передачи данных Ленинградской области №6440**;

- Secret Net 7

- Антивирус Kaspersky Internet Security

**(расчет стоимости и контакты в Приложении № 1);**

2) разработать и утвердить организационно-распорядительные документы в соответствии с постановлением правительства Ленинградской области от 11.09.2015 № 358 «Об утверждении типовых организационно-распорядительных документов операторов персональных данных»

**(типовые документы в Приложении № 2);**

3) разработать и утвердить организационно-распорядительные документы по защите информации **(типовые документы в Приложении № 3).**

**ПОЯСНЕНИЯ**

**1.** Для выполнения обязанностей операторов персональных данных по организации обработки персональных данных, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (152-ФЗ), необходимо самостоятельно определить состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, в том числе:

1) назначить, ответственного за организацию обработки персональных данных;

2) направить в территориальный орган Роскомнадзора уведомление об обработке персональных данных;

3) издать, документы, определяющие политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

4) применять правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со ст. 19 152-ФЗ;

5) осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

6) оценить вред, который может быть причинен субъектам персональных данных в случае нарушения 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ;

7) ознакомить работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператор в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

8) выполнить иные мероприятия предусмотренные 152-ФЗ.

**2.** Для обеспечения безопасности информации на автоматизированных рабочих местах (АРМ) государственной информационной системы Ленинградской области «Контингент-ЛО» (ИС «Контингент-ЛО»), необходимо выполнить следующие мероприятия:

1. в соответствии с п. 15 ПП РФ № 1119, п. 9 «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утверждённым приказом ФСТЭК России от 11.02.2013 № 17 (Приказ ФСТЭК России № 17), п. 17 «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», утверждённых приказом ФСБ России от 10.07.2014 № 378 (Приказ ФСБ России № 378) для обеспечения защиты персональных данных, назначить структурное подразделение или должностное лицо (работник), ответственных за защиту информации;

2. в соответствии с п. 15 ПП РФ № 1119:

а) организовать режим обеспечения безопасности помещений, в которых размещены АРМ ИС «Контингент-ЛО», препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечить сохранность носителей персональных данных;

в) утвердить документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым на АРМ ИС «Контингент-ЛО», необходим для выполнения ими служебных (трудовых) обязанностей;

г) использовать средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;

3. в соответствии с п. 15 ПП РФ № 1119:

необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;

4. в соответствии с п. 6. Приказ ФСБ России № 378:

для выполнения требования, указанного в пп. а) п. 15 ПП РФ № 1119, необходимо обеспечение режима, препятствующего возможности неконтролируемого проникновения или пребывания в помещениях, где размещены используемые средства криптографической защиты информации (СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее - Помещения), лиц, не имеющих права доступа в Помещения, которое достигается путем:

а) оснащения Помещений входными дверьми с замками, обеспечения постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений;

б) утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

в) утверждения перечня лиц, имеющих право доступа в Помещения;

для выполнения требования, указанного в подпункте б) п. 15 ПП РФ № 1119 необходимо:

а) осуществлять хранение съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов);

б) осуществлять поэкземплярный учет машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров;

для выполнения требования, указанного в подпункте в) п. 15 ПП РФ № 1119 необходимо внедрить соответствующие СКЗИ

а) разработать и утвердить документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым на АРМ ИС «Контингент-ЛО», необходим для выполнения ими служебных (трудовых) обязанностей;

б) поддерживать в актуальном состоянии документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым на АРМ ИС «Контингент-ЛО», необходим для выполнения ими служебных (трудовых) обязанностей;

для выполнения требования, указанного в подпункте г) п. 15 ПП РФ № 1119 необходимо внедрить соответствующие средства криптографической защиты информации;

для выполнения требования, указанного в п. 15 ПП РФ № 1119, необходимо:

а) утверждение руководителем оператора списка лиц, допущенных к содержанию электронного журнала сообщений, и поддержание указанного списка в актуальном состоянии;

б) обеспечение АРМ ИС «Контингент-ЛО» автоматизированными средствами, регистрирующими запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам в электронном журнале сообщений;

в) обеспечение АРМ ИС «Контингент-ЛО» автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного журнала сообщений;

г) обеспечение периодического контроля работоспособности указанных в подпунктах «б» и «в» настоящего пункта автоматизированных средств (не реже 1 раза в полгода);

5. в соответствии с Приказом ФСТЭК России № 17, с учётом документации, разработанной документации, переданной Комитету экономического развития (письмо от 20.11.2015 № 022-3495/15-0-1), необходимо произвести:

установку и настройку средств защиты информации на АРМ ИС «Контингент-ЛО»;

разработку документов для реализации оператором обеспечения защиты информации на АРМ ИС «Контингент-ЛО» в ходе ее эксплуатации, определяющие правила и процедуры:

- управления (администрирования) системой защиты информации АРМ ИС «Контингент-ЛО»;

- выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования АРМ ИС «Контингент-ЛО» и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;

- управления конфигурацией системы защиты информации АРМ ИС «Контингент-ЛО»;

- контроля (мониторинга) за обеспечением уровня защищенности информации АРМ ИС «Контингент-ЛО»;

внедрение организационных мер защиты информации;

аттестацию АРМ ИС «Контингент-ЛО» по требованиям безопасности информации.