Действующая редакция (без изменений и дополнений)

ПРАВИТЕЛЬСТВО
ПРИДНЕСТРОВКОЙ МОЛДАВСКОЙ РЕСПУБЛИКИ

ПОСТАНОВЛЕНИЕ

5 августа 2014 года № 206

Об утверждении требований
к защите персональных данных
при обработке в информационных системах
персональных данных

В соответствии со статьей 76-6 Конституции Приднестровской Молдавской Республики, Конституционным законом Приднестровской Молдавской Республики от 30 ноября 2011 года № 224-КЗ-V «О Правительстве Приднестровской Молдавской Республики» (САЗ 11-48) с дополнением, внесенным Конституционным законом Приднестровской Молдавской Республики от 26 октября 2012 года № 206-КЗ-V (САЗ 12-44), Законом Приднестровской Молдавской Республики от 16 апреля 2010 года № 53-З-IV «О персональных данных» (САЗ 10-15) с изменениями и дополнениями, внесенными законами Приднестровской Молдавской Республики от 5 декабря 2013 года № 257-ЗИД-V (САЗ 13-48), от 21 января 2014 года № 19-ЗИ-V (САЗ 14-4), Правительство Приднестровской Молдавской Республики
п о с т а н о в л я е т:

1. Утвердить Требования к защите персональных данных при их обработке в информационных системах персональных данных (прилагаются).

2. Настоящее Постановление вступает в силу со дня признания утратившим силу Указа Президента Приднестровской Молдавской Республики от 20 мая 2013 года № 224 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (САЗ 13-20).

3. Ответственность за реализацию настоящего Постановления возложить на начальника Государственной службы связи, информации и СМИ Приднестровской Молдавской Республики.

4. Контроль за исполнением настоящего Постановления возложить на заместителя Председателя Правительства Приднестровской Молдавской Республики – председателя Комитета цен и антимонопольной деятельности Приднестровской Молдавской Республики.

ПРЕДСЕДАТЕЛЬ ПРАВИТЕЛЬСТВА Т.ТУРАНСКАЯ

ПРИЛОЖЕНИЕ
к Постановлению Правительства
Приднестровской Молдавской
Республики
от 5 августа 2014 года № 206

ТРЕБОВАНИЯ
к защите персональных данных при их обработке в информационных системах персональных данных

1. Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее – информационные системы) и уровни защищенности таких данных.

2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с пунктом 5 статьи 19 Закона Приднестровской Молдавской Республики от 16 апреля 2010 года № 53-З-IV «О персональных данных» (САЗ 10-15) (далее – Закон Приднестровской Молдавской Республики «О персональных данных»).

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее – оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица соблюдать конфиденциальность в отношении персональных данных и обеспечение безопасности персональных данных при их обработке в информационной системе.

4. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми уполномоченным органом по защите прав субъектов персональных данных и уполномоченным Президентом Приднестровской Молдавской Республики исполнительным органом государственной власти в сфере государственной безопасности, в пределах их полномочий, во исполнение пункта 4 статьи 19 Закона Приднестровской Молдавской Республики «О персональных данных».

5. Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Закона Приднестровской Молдавской Республики «О персональных данных».

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в первой, второй и третьей частях настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

6. 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, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1 типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2 типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3 типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

7. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение подпункта «д» пункта 1 статьи 18-1 Закона Приднестровской Молдавской Республики «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение пункта 5 статьи 19 Закона Приднестровской Молдавской Республики «О персональных данных».

8. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

9. Необходимость обеспечения 1 уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1 типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2 типа и информационная система обрабатывает специальные категории персональных данных более чем 5000 субъектов персональных данных, не являющихся сотрудниками оператора.

10. Необходимость обеспечения 2 уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2 типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 5000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2 типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2 типа и информационная система обрабатывает общедоступные персональные данные более чем 5000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2 типа и информационная система обрабатывает иные категории персональных данных более чем 5000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3 типа и информационная система обрабатывает специальные категории персональных данных более чем 5000 субъектов персональных данных, не являющихся сотрудниками оператора.

11. Необходимость обеспечения 3 уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2 типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 5000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2 типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 5000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3 типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 5000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3 типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3 типа и информационная система обрабатывает иные категории персональных данных более чем 5000 субъектов персональных данных, не являющихся сотрудниками оператора.

12. Необходимость обеспечения 4 уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3 типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 5000 субъектов персональных данных, не являющихся сотрудниками оператора.

13. Для обеспечения 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности

неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

14. Для обеспечения 3 уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

15. Для обеспечения 2 уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 14 настоящего документа, 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.

16. Для обеспечения 1 уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 15 настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

17. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе лиц, имеющих лицензию на осуществление деятельности по оказанию услуг по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).