УТВЕРЖДЕНО

приказом комитета
Ставропольского края
по делам архивов
от 31.12.2013 № 147

Положение
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных комитета Ставропольского края по делам архивов

1. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных комитета Ставропольского края по делам архивов (далее – комитет), представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах персональных данных.

Персональные данные (далее – ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, субъекту ПДн.

Оператор ПДн – комитет, обеспечивающий защиту ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2. Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн.

Безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью системы защиты ПДн, включающей организационные меры и средства защиты информации (далее – СЗПДн) (в том числе шифровальные (криптографические), средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в ИСПДн информационные технологии. Технические и программные средства должны удовлетворять требованиям действующего законодательства.

3. ИСПДн классифицируются в зависимости от объема обрабатываемых ПДн и угроз безопасности жизненно важным интересам личности, общества и государства.

Порядок проведения классификации ИСПДн устанавливается в соответствии с действующим законодательством.

4. Обмен ПДн при их обработке в ИСПДн осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

5. Размещение ИСПДн производится в специальном оборудованном помещении, в котором обеспечивается сохранность носителей ПДн и СЗПДн, а также исключена возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

6. При обработке ПДн в ИСПДн должно быть обеспечено:

проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн, и (или) передачи их лицам, не имеющим права доступа к такой информации;

своевременное обнаружение фактов несанкционированного доступа к ПДн;

недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

постоянный контроль за обеспечением уровня защищенности ПДн.

7. Мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн включают в себя:

определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;

разработку на основе модели угроз СЗПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;

проверку готовности СЗПДн к использованию с составлением заключений о возможности их эксплуатации;

установку и ввод в эксплуатацию СЗПДн в соответствии с эксплуатационной и технической документацией;

обучение лиц, использующих СЗПДн, применяемые в ИСПДн, правилам работы с ними;

учет применяемых СЗПДн, эксплуатационной и технической документации к ним, носителей ПДн;

учет лиц, допущенных к работе с ПДн в ИСПДн;

контроль за соблюдением условий использования СЗПДн, предусмотренных эксплуатационной и технической документацией;

описание СЗПДн.

8. Запросы пользователей ИСПДн на получение ПДн, а также факты предоставления ПДн по этим запросам регистрируются автоматизированными средствами ИСПДн в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется администратором информационной безопасности ИСПДн или ответственным за защиту

информации и ПДн комитета, назначаемыми приказами комитета.

9. При обнаружении нарушений порядка предоставления ПДн пользователи ИСПДн незамедлительно приостанавливают предоставление ПДн до выявления причин нарушений и устранения этих причин.

10. Реализация требований по обеспечению безопасности информации в СЗПДн возлагается на их разработчиков.

11. СЗПДн, предназначенные для обеспечения безопасности ПДн при их обработке в ИСПДн, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется действующим законодательством.