Требования ФСБ России к обеспечению безопасности персональных данных с использованием средств криптографической защиты информации

Владивосток, 2017

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности
№ 149/7/2/6-432 от 31 марта 2015 года

Использование СКЗИ для обеспечения безопасности персональных данных необходимо в следующих случаях:

- если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;
- если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

К случаям, когда угрозы могут быть нейтрализованы только с помощью СКЗИ, относятся:

- **передача персональных данных по каналам связи**, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию;
- **хранение персональных данных на носителях информации**, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

Нормативно-методические документы ФСБ России, действующие в области обеспечения безопасности персональных данных

Приказ ФСБ России
от 10 июля 2014 года № 378

«Об утверждении 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»

Приказ ФСБ России
от 9 февраля 2005 года № 66
«Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»

«Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная **приказом ФАПСИ от 13 июня 2001 года № 152**

Основные требования к применению СКЗИ:

- СКЗИ должны быть сертифицированы;
- класс используемого СКЗИ должен обеспечивать нейтрализацию установленных угроз;

Перечень средств защиты информации, сертифицированных ФСБ России, представлен на сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России

clsz.fsb.ru

Основные требования к применению СКЗИ:

- СКЗИ должны приобретаться у лицензиатов ФСБ России;
- на месте эксплуатации СКЗИ должны быть в наличии дистрибутивы, формуляры и правила пользования;
- СКЗИ должны быть учтены в соответствии с учетными номерами, присваиваемыми ФСБ России;

Основные требования к применению СКЗИ:

- пользователи СКЗИ должны быть обучены правилам работы с отметками в журнале учета пользователей СКЗИ;
- в процессе эксплуатации СКЗИ необходимо внимательно относиться к выполнению требований и условий, указанных в формуляре и правилах пользования.

В формулярах зачастую присутствуют требования по использованию средств доверенной загрузки, антивирусных и иных средств защиты для достижения заданного класса криптографической защиты, а также необходимость внесения изменений в реестр для корректной работы СКЗИ.

Обобщенные результаты проверок обеспечения безопасности персональных данных при их обработке в ИСПДн, проведенных ФСБ России в 2016 году

По итогам контрольных мероприятий, проведенных в отношении 541 оператора персональных данных

- 53% - работали без нарушений или с незначительными отступлениями от требований нормативных документов;

- в отношении 47% - были применены меры административного воздействия, .

Спасибо за внимание!