Обзор приказа ФСТЭК РФ от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

Положения вступившего в силу постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» гласят о том, что выбор средств защиты информации для системы защиты персональных данных должен осуществляться оператором в соответствии с нормативными правовыми актами ФСТЭК России и ФСБ России. Один из таких актов, а именно приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее - П-21), был принят в соответствии с частью 4 статьи 19 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных». Что касается требований, связанных с применением шифровальных средств защиты информации, то они регламентируются приказом ФСБ России от 10.07.2014 № 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».

В соответствии с информационным сообщением ФСТЭК России от 20.11.2012 г. № 240/24/4669 «Об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных», П-21 применяется к информационным системам персональных данных, для которых решение о создании системы защиты информации будет принято после вступления его в силу, т.е. после 02.06.2013.

П-21 отменил действие приказа ФСТЭК России от 05.02.2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных», согласно которому выбор и реализация методов и способов защиты информации в информационной системе

должны были осуществляться на основе определяемых оператором (уполномоченным лицом) угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы. Согласно П-21 принимаемые операторами меры по обеспечению безопасности персональных данных должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных. В приложении к П-21 приведены конкретные составы и содержание мер по обеспечению безопасности персональных данных, необходимые для обеспечения каждого из уровней защищенности персональных данных.

При выборе мер по обеспечению безопасности персональных данных оператору необходимо:

- определить базовый набор мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с приложением;
- адаптировать этот базовый набор мер с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы;
- провести уточнение адаптированного базового набора мер с учетом не выбранных ранее мер, по результатам которого определить меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;
- дополнить уточненный адаптированный базовый набор мер мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

В п.10 П-21 также оговаривается, что если оператор не имеет возможности технической реализации отдельных выбранных мер, а также учитывая экономическую целесообразность на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер, оператор вправе разработать иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных, и обосновать их применение. Компенсирующие меры должны разрабатываться операторами также при использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональных данных, для которых не определены меры обеспечения их безопасности.

Операторам, использующим в информационных системах сертифицированные по требованиям безопасности информации средства защиты, необходимо руководствоваться положениями п.12 П-21, в которых четко определено, какие средства вычислительной техники, системы обнаружения вторжений, средства антивирусной защиты, межсетевые экраны необходимо применять для обеспечения каждого из уровней защищенности персональных данных.

Оценивать эффективность реализации принимаемых мер оператору необходимо не реже 1 раза в 3 года либо своими силами, либо привлекая лицензиатов ФСТЭК России.

Таким образом, концепция выполнения положений П-21 выглядит следующим образом:

- разработка перечня актуальных угроз;
- определение уровней защищенности персональных данных;
- определение базовых мер по обеспечению безопасности персональных данных, которые необходимо применять для обеспечения каждого из уровней защищенности;
- оценка применимости базовых мер;
- при необходимости - определение перечня компенсирующих мер, которые способны нейтрализовать актуальные угрозы безопасности, и их обоснование.