



**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)**

ДИРЕКТОР

Старая Басманная, д. 17, Москва, 105175
Тел., факс (495) 696-49-04
E-mail: postin@fstec.ru

12.06.2013 № 240/22/2221

На № _____

Члену Совета Федерации
Федерального Собрания Российской Федерации

Р.У.ГАТТАРОВУ

ул. Б. Дмитровка, д. 26,
Москва, 103426

О требованиях по информационной
безопасности ФЦОД ЕГИСЗ Минздрава России

Уважаемый Руслан Усманович!

Вопросы об угрозах безопасности информации в Единой государственной информационной системе в сфере здравоохранения (далее – информационная система Минздрава России), соответствия созданных элементов информационной системы нормативным требованиям по информационной безопасности и согласования проектных решений и документации на информационную систему ФСТЭК России рассмотрены.

В ходе рассмотрения указанных вопросов проведен анализ «Документации об открытом аукционе в электронной форме на право заключения государственного контракта на выполнение работ по проектированию и организации телекоммуникационных и вычислительных мощностей Федерального центра обработки данных (ФЦОД ЕГИСЗ) Министерства здравоохранения Российской Федерации (основная, резервная и тестовая площадки) и оказание услуг по организации телекоммуникационной инфраструктуры защищенных каналов связи между основной и резервной площадками ФЦОД ЕГИСЗ Министерства здравоохранения Российской Федерации, в которых размещены компоненты ЕГИСЗ и узлами доступа субъектов Российской Федерации, а также сопровождение и эксплуатация ФЦОД ЕГИСЗ Министерства здравоохранения Российской Федерации и прикладных компонентов ЕГИСЗ», размещенной на сайте www.zakupki.gov.ru.

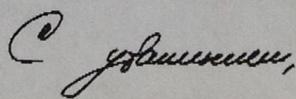
Анализ аукционной документации показал, что в ней в целом определены требования по информационной безопасности при проектировании Федерального центра обработки данных информационной системы Минздрава России, а также при оказании услуг по эксплуатации его инфраструктуры. В частности установлены требования к реализации системы организационных, технических и

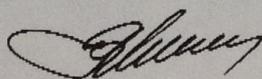
других мер, направленных на обеспечение информационной безопасности в соответствии с требованиями действующего законодательства Российской Федерации, нормативных правовых актов и методических документов ФСБ России и ФСТЭК России по защите информации, определена необходимость наличия политики информационной безопасности, модели угроз безопасности информации и модели нарушителя, предъявлены требования к аттестации отдельных сегментов информационной системы, а также к использованию средств защиты информации, сертифицированных по требованиям безопасности информации ФСТЭК России и ФСБ России в пределах компетенции.

Вместе с тем согласно аукционной документации для обеспечения инвариантности инфраструктуры и обеспечения отказоустойчивости и катастрофоустойчивости технологическая база Федерального центра обработки данных информационной системы Минздрава России должна строиться на базе виртуальной инфраструктуры. Таким образом, при создании информационной системы будут использованы технологии виртуализации, которые обуславливают возникновение новых классов угроз безопасности информации (например, неконтролируемую миграцию виртуальных машин и данных, выход обработки данных за пределы виртуальных машин) и определяют дополнительные требования к обеспечению защиты информации от несанкционированного доступа. Указанные угрозы безопасности информации при формировании требований по информационной безопасности не учтены.

Размещение центральной базы информационной системы Минздрава России, являющейся государственной информационной системой, на инфраструктуре коммерческих операторов центров обработки данных возможно исключительно в случаях соответствия этих центров обработки данных требованиям нормативных правовых актов по защите информации, содержащейся в государственных информационных системах. При этом должно быть обеспечено выполнение Минздравом России требований части 4 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в том числе в части контроля за уровнем защищенности информации, обрабатываемой на инфраструктуре коммерческих операторов. Анализ аукционной документации показал, что указанные требования в ней не предусмотрены.

Одновременно сообщаю, что модель угроз безопасности информации, проектные решения и иная документация на Федеральный центр обработки данных информационной системы Минздрава России в ФСТЭК России на рассмотрение не поступали.





В.Селин