Н.А. Самоделова,
специалист B2B

Сетевая безопасность.
Изучение технических заданий – эквивалент недопустим?

В статье рассказывается о требованиях, которым должны соответствовать средства криптографической защиты информации, какими ГОСТами и другими нормативными правовыми актами они устанавливаются. Автор объясняет, что такое совместимость, какой она бывает, в каких случаях нужна техническая, а в каких – и техническая, и функциональная совместимость. На примерах технических заданий показано, что почти во всех случаях заказчики устанавливают такие требования, которым отвечает только одно конкретное СКЗИ.

Требования к СКЗИ и их сертификации

Анализ технических заданий аукционов на предмет эквивалентности закупаемых средств криптографической защиты информации (СКЗИ) показывает, что даже порядок исполнения обязательств в рамках законодательства о закупках вольно или невольно приводит в некоторых случаях к завуалированному ограничению конкуренции. Документация о закупке, в состав которой включено техническое задание, размещается на официальном сайте. С момента размещения эта информация становится доступной неограниченному кругу лиц, и участник аукциона для формирования своего предложения может проверить обоснованность установленных требований в техническом задании, как самостоятельно проверив это задание, так и обратившись в экспертную организацию.

Нормативно-правовые акты Российской Федерации, устанавливающие требования к защите персональных данных, в частности при передаче их по открытым каналам связи, не определяют конкретных средств защиты информации, которые должны использоваться с этой целью. Они определяют лишь, что выбор таких средств должен осуществляться

оператором в соответствии с нормативно-правовыми актами, принятыми ФСБ России и ФСТЭК России во исполнение ч. 4 ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Кроме того, предъявляются требования к средствам защиты информации в части прохождения в установленном порядке процедуры оценки соответствия, которая для криптографических средств заключается в процедуре сертификации на соответствие требованиям ФСБ России, а для межсетевых экранов – сертификации на соответствие требованиям ФСТЭК России и (или) на соответствие требованиям ФСБ России.

В некоторых случаях необходимо руководствоваться еще и приказом Минкомсвязи России от 09.12.2013 № 390 (далее – Приказ № 390), который определяет правила присоединения информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме. В Приказе № 390 предъявляются требования к защите каналов связи, а также закрепляется уровень класса защиты для подобных систем: защита должна быть осуществлена средствами криптографической защиты, сертифицированными по классу не ниже КС3. Согласно тому же приказу межсетевые экраны, обеспечивающие контроль за информацией, поступающей в информационную систему, должны быть сертифицированы по требованиям ФСБ России к устройствам типа «межсетевые экраны» по четвертому классу защищенности. А по требованиям ФСТЭК России к устройствам типа «межсетевые экраны» – по третьему классу и третьему уровню контроля отсутствия недекларированных возможностей.

Выбор конкретных средств защиты разработчиком системы производится на этапе проектирования подсистемы безопасности, исходя из возможности нейтрализации угроз безопасности информации, признанных актуальными для конкретных условий функционирования системы. При необходимости готовится технико-экономическое обоснование их использования, а также детально рассматриваются все вопросы совместимости (технической и функциональной) включаемых в состав информационной системы технических средств.

Пункт 1 ч. 1 ст. 33 Закона о контрактной системе (так же как и ч. 2 ст. 34 Закона № 94-ФЗ) обязывает заказчика устанавливать в документации об аукционе в электронной форме требования к функциональным, техническим, качественным, эксплуатационным характеристикам объекта закупки, разрешая использовать ссылку на товарные знаки только в случае, если не имеется другого способа, обеспечивающего более точное и четкое описание характеристик объекта закупки. Документация о закупке может содержать указание на товарные знаки в случае, если при выполнении работ, оказании услуг предполагается использовать товары, поставки которых не являются предметом контракта. При этом обязательным условием является включение в описа-

ние объекта закупки слов «или эквивалент», за исключением случаев несовместимости товаров, на которых размещаются другие товарные знаки, и необходимости обеспечения взаимодействия таких товаров с товарами, используемыми заказчиком.

Следовательно, любой заказчик вправе установить требования к поставляемым товарам таким образом, чтобы они соответствовали его потребностям. Более того, Закон о контрактной системе не содержит положений, которые бы обязывали заказчика устанавливать требования к поставляемым товарам, которым бы отвечало максимальное количество наименований какой бы то ни было продукции, в т. ч. средств защиты информации.

Не умаляя права заказчика самостоятельно определять собственные потребности при осуществлении закупки, в том числе в виде определенных требований к предмету закупки, установление которых направлено на получение по итогам определения поставщика качественного товара, законодатель ограничивает такое право, не допуская установления требований, влекущих за собой ограничение количества участников такого аукциона или ограничение доступа к участию в таком аукционе.

Арбитражные суды при рассмотрении исков по оценке правомерности установленных требований в документации рассматривают всю совокупность сведений о закупаемом товаре: представлены ли сведения о наличии на рынке нескольких производителей, поставщиков требуемого товара, обусловлены ли требования к товару необходимостью обеспечения взаимодействия закупаемых товаров с оборудованием, имеющимся у заказчика, и нормами законодательства, влекут ли требования ограничение числа участников закупки, поданы ли на участие заявки и имеются ли запросы от участников закупки.

Понятие совместимости

Законодательство Российской Федерации, в частности Закон о контрактной системе, не дает четкого определения совместимости продуктов. Эту задачу выполняет заказчик, выдвигая в соответствии с п. 1 ч. 1 ст. 33 Закона о КС требования к техническим характеристикам товаров, их безопасности и функциональным характеристикам и оценивая соответствие предлагаемых участниками аукциона товаров заявленным требованиям.

На российском рынке в настоящее время представлено достаточно много сертифицированных СКЗИ различных производителей, предназначенных для выполнения одинаковых базовых функций – защиты информации, передаваемой по не заслуживающим доверия каналам. Все СКЗИ обеспечивают защиту передаваемой информации с использованием алгоритмов, соответствующих ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» и ГОСТ Р 34.10-2001 «Информацион-

ная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

СПРАВОЧНО

Хотелось бы сразу обратить внимание, что, несмотря на то что указанный ГОСТ утратил силу в связи с изданием приказа Росстандарта от 07.08.2012 № 215, которым утвержден новый ГОСТ Р 34.10-2012, существует порядок перехода на новый стандарт, опубликованный на сайте технического комитета по стандартизации (ТК-26) *http://tc26.ru/info/34.10-2012_34.11-2012/*, согласно которому использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи не допускается только после 31 декабря 2018 г.

Все эти средства сертифицированы ФСБ России (*http://clsz.fsb.ru/files/download/svedeniya_po_sertifikatam_01122013.doc*) и ФСТЭК России и могут применяться для защиты персональных данных в различных информационных системах.

Именно от того, как заказчик составит требования эквивалентности, зависит возможность участия разных производителей СКЗИ в аукционе. Если рассматривать понятие «эквивалентность» с точки зрения назначения средств защиты информации и решаемых задач (техническую совместимость), то СКЗИ различных компаний эквивалентны. Однако если рассматривать понятие «эквивалентность» с точки зрения функциональной совместимости (протоколы, интерфейсы), то *СКЗИ производства любых разных компаний не являются эквивалентными.*

СПРАВОЧНО

В ГОСТ Р ИСО/ТО 16056-1-2009 «Информатизация здоровья. Функциональная совместимость систем и сетей телездравоохранения» в части 1, в определениях функциональная совместимость определяется следующим образом: «Под функциональной совместимостью понимается способность двух и более систем (компьютеров, коммуникационных устройств, сетей, программного обеспечения и других компонентов информационных технологий) взаимодействовать друг с другом и обмениваться информацией в соответствии с установленной процедурой для достижения предсказуемых результатов».

Отсюда следует, что для средств защиты информации *функциональная совместимость* означает *возможность встречной работы*.

Имеется единственный ГОСТ 30709-2002 «Техническая совместимость. Термины и определения», который дает определение технической совместимости изделий различного назначения:

«3.1. Совместимость: пригодность продукции, процессов или услуг к совместному, но не вызывающему нежелательных взаимодействий использованию при заданных условиях для выполнения установленных требований;

3.2. Техническая совместимость: совместимость изделий, их составных частей, конструкционных, горюче-смазочных материалов, технологических процессов изготовления и контроля».

Исходя из этого определения, *техническая совместимость* средств защиты информации (СЗИ) означает возможность *совместного использования без встречной работы*, а просто в одной сети.

Поэтому нельзя рассматривать вопрос выбора тех или иных средств защиты информации (СЗИ) в отрыве от задачи построения информационной системы (ИС) в целом, так как закупка СЗИ в рамках аукциона в электронной форме осуществляется, как правило, для построения сегмента ИС. Проводить анализ функциональной и технической совместимости СЗИ необходимо именно на уровне подсистем (или сегментов) одной информационной системы заказчика. СЗИ различных производителей на уровне взаимодействия подсистем (сегментов) одной информационной системы технически совместимы, т. к. не оказывают взаимного негативного воздействия друг на друга, а их одновременное использование не влияет на выполнение ими своих функций – криптографическую защиту информации, передаваемой по открытым каналам связи в соответствии с требованиями федеральных органов исполнительной власти, уполномоченных в области безопасности и технической защиты информации (ФСБ России и ФСТЭК России).

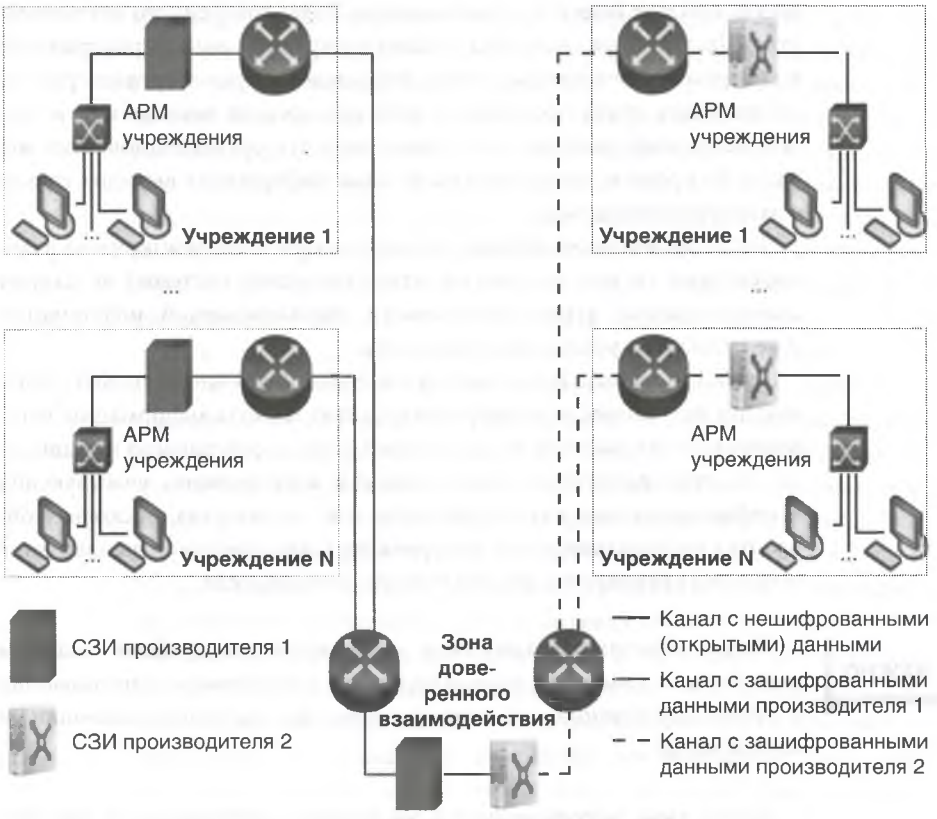
Типы закупки СЗИ. Примеры

Однако, проанализировав технические задания на закупку средств защиты информации, приходим к выводу, что СЗИ при построении сегментов Единых государственных информационных систем, извещения о которых размещены на официальном сайте, в рамках темы эквивалентности (совместимости) условно можно классифицировать следующим образом:

- закупка СЗИ для нового сегмента ИС. В данном случае достаточно говорить только о технической совместимости вновь закупаемых СЗИ с уже имеющимися в других сегментах;
- закупка СЗИ в уже созданный сегмент, с установленными в нем ранее средствами защиты информации. В таком случае обязательно необходимо рассматривать и техническую, и функциональную совместимость вновь закупаемых СЗИ с уже установленными в данном сегменте.

Попробуем разобрать на примерах. Хотелось бы сразу оговориться, что приведенные примеры не являются исключением, а всего лишь наглядно демонстрируют распространенные типы технических заданий на закупку СЗИ, опубликованные на официальном сайте. Все заказчики, уже проведшие подобные торги, могут попробовать сами определить, к какому типу можно отнести их техническое задание.

Итак, в извещении № 0116300000113000400 требования к СЗИ, описанные в техническом задании, звучат следующим образом: «Должны иметь возможность интеграции с имеющимися средствами криптографической защиты информации, используемыми в системе межведомственного и межуровневого электронного документооборота». Можно уже на данном этапе определить, что СЗИ закупаются *для нового сегмента*.



Совместная работа СЗИ различных производителей

В данном случае возможна закупка СЗИ различных производителей. Это доступно объясняется Минздравом России в документации, описывающей различные варианты построения Единой государственной информационной системы здравоохранения (ЕГИСЗ) «Подключение к VPN сети ЕГИСЗ.pdf» (*http://egisz.rosminzdrav.ru/ вкладка «Документы»/переход на страницу 6*), где приводится пример одного из возможных вариантов совместного использования СЗИ двух разных производителей (рисунок).

В этом примере информационное взаимодействие двух систем (подсистем, сегментов одной системы), использующих средства криптографической защиты информации различных производителей, обеспечивается техническими средствами путем создания зоны доверенного взаимодействия (шлюза), обеспечивающего дешифрование информации, получаемой от одного аппаратного программного комплекса, и шифрование с использованием другого. Таким образом, на рабочее место пользователя данные доставляются в виде, обеспечивающем возможность их расшифровывания с использованием того средства за-

щиты, которое имеется у пользователя. Зоны доверенного взаимодействия (шлюзы) размещаются в контролируемой зоне (пространстве, в котором не допускается пребывание людей и транспортных средств, не имеющих права постоянного или разового их посещения), и безопасность информации в них обеспечивается организационными мерами. За пределы контролируемой зоны информация выходит только в зашифрованном виде.

Такая организация обработки данных при информационном взаимодействии систем (подсистем сегментов одной системы) не создает дополнительных угроз безопасности обрабатываемой информации и не снижает ее уровня защищенности.

Удобство работы пользователя системы обусловлено только степенью дружественности интерфейса средства защиты информации, установленного на рабочем месте пользователя, и совершенно не зависит от наличия различных систем защиты информации, участвующих в информационном взаимодействии, и их количества, поскольку обработка информации в зоне доверенного взаимодействия выполняется полностью автоматически, без участия пользователя.

ВАЖНО!

Таким образом, техническая совместимость средств защиты информации означает возможность их совместного использования в одной информационной сети/системе без взаимного негативного воздействия.

Кроме того, использование СЗИ разных производителей при построении подсистемы информационной безопасности, несмотря на некоторое усложнение технической инфраструктуры, позволяет заказчику существенно снизить риски зависимости от единственного (монопольного) поставщика СЗИ (отказ от поставки, отказ от техподдержки, качество сервисов, стоимость СЗИ и сервисов и т. д.), а также привести к снижению цен и экономии бюджетных средств при проведении аукциона.

В связи со сказанным в качестве примера можно привести результаты аукциона № 0165200000512000907 на «поставку маршрутизаторов и программно-аппаратных комплексов средств криптографической защиты информации с оказанием услуг по преднастройке, инструктажу персонала по базовому конфигурированию оборудования, настройке и поиску неисправностей» с начальной максимальной ценой контракта 13 782 593,10 руб. В конкурентной борьбе за право заключения контракта участвовали пять участников размещения заказа с продукцией двух разных производителей. В результате аукционной борьбы между участниками размещения заказа цена контракта снизилась и составила 11 802 218,42 руб.

В извещении № 0361200014413000093 требования к СКЗИ в техническом задании описаны так: «Использование эквивалента недопустимо

во избежание несовместимости с программно-аппаратными комплексами, установленными для защиты каналов связи системы межведомственного электронного взаимодействия области *и использующимися на оборудовании* заказчика». Безусловно, в данном случае необходимо рассматривать уже не только техническую, но и функциональную совместимость, и в этом случае необходимо докупать средства защиты информации той же торговой марки, которые уже стоят в ИС заказчика в данном сегменте, поскольку, как писалось выше, *СЗИ производства любых разных компаний не являются эквивалентными, т. к. функционально* (протоколы, интерфейсы) несовместимы.

Есть третья разновидность формулировок требований к СЗИ, когда в техническом задании указывается торговая марка СЗИ и дополняется словами «или эквивалент». (Примеры можно посмотреть в технических заданиях извещений № 0173100009713000490, 0347200001413001430.) С точки зрения как Закона о контрактной системе, так и Закона № 94-ФЗ подобные формулировки допустимы. Формальности соблюдены. И, несмотря на то что согласно п. 1 ч. 3 ст. 66 Закона о контрактной системе в таких случаях необходимо либо согласие участника такого аукциона на поставку товара в случае, если этот участник предлагает для поставки товар, в отношении которого в документации о таком аукционе содержится указание на товарный знак, либо конкретные показатели товара, соответствующие значениям эквивалентности, установленным данной документацией, если такой участник предлагает для поставки товар, который является эквивалентным товару, указанному в данной документации, фактически в таких аукционах предлагается и закупается продукция именно указанной торговой марки, поскольку приведенные функциональные характеристики соответствуют только ей. Как уже говорилось, *СЗИ производства любых разных компаний не являются эквивалентными, т. к. функционально несовместимы.*

Безусловно, когда в данную подсеть будет поставлено оборудование указанной торговой марки и возникнет необходимость дальнейшего ее расширения, в техническом задании будет прописано: «Использование эквивалента недопустимо во избежание несовместимости с программно-аппаратными комплексами, *использующимися на оборудовании* заказчика» (пример – извещение № 0151200001613000258).

Таким образом, закупка средств защиты информации фактически вне зависимости от формулировок технического задания и соблюдения норм законодательства в своем большинстве всегда означает, что «эквивалент недопустим», даже если написано «или эквивалент».