Подключаемся к СМЭВ[1]: выбор криптооборудования

В конце 2015 г. Минсвязи России в рамках работ по развитию Единой системы межведомственного электронного взаимодействия (СМЭВ) расширило перечень криптографического оборудования, с помощью которого можно подключиться к инфраструктуре электронного правительства, включив в него продукты компании «С-Терра СиЭсПи».

Н.А. Самоделова,
руководитель отдела анализа госзакупок компании «С-Терра СиЭсПи»

Создание системы межведомственного электронного взаимодействия (далее – СМЭВ) решило важный и актуальный вопрос современного общества – обеспечило возможность организации оперативного информационного взаимодействия федеральных и региональных органов исполнительной власти, органов местного самоуправления и ряда иных структур между собой. Это позволило обеспечить исполнение органами власти различных уровней возложенных на них функций в электронном виде, а также максимально упростило процедуру получения государственных и муниципальных услуг, дав возможность предоставлять их в электронной форме, используя, по сути, принцип «одного окна», что, собственно, и являлось целью создания СМЭВ. Постановлением Правительства РФ от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия» государственным заказчиком и оператором СМЭВ определено Минкомсвязи России, а распоряжением Правительства РФ от 15.10.2009 № 1475-р утвержден единственный исполнитель работ по эксплуатации инфраструктуры электронного правительства – единый национальный оператор инфраструктуры электронного правительства – ПАО «Ростелеком».

Требования к организации работы в СМЭВ довольно обширны, они подробно описаны на специализированном технологическом портале. Остановимся на одном аспекте – **использовании криптографического оборудования для защиты информации**, циркулирующей в системе, поскольку передача в сети персональных данных и иной конфиденциальной информации накладывает определенные технические требования к защите каналов связи[2].

[1] СМЭВ – система межведомственного электронного взаимодействия.

[2] Приказ Минкомсвязи России от 23.06.2015 № 210 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия»

Проблема совместимости решена

Первоначально участниками СМЭВ были исключительно организации разных уровней, предоставляющие государственные и муниципальные услуги. Для защиты каналов связи заказчиком было выбрано оборудование одного производителя, которое предоставлялось федеральным органам исполнительной власти (ФОИВ) во временное пользование.

Но с развитием СМЭВ и введением Государственной информационной системы о государственных и муниципальных платежах в систему взаимодействия были включены управляющие бюджетными средствами кредитно-финансовые организации с уже организованной защищенной информационной сетью. Причем зачастую использовались в ней средства шифрования иных производителей (например, «С-Терра СиЭсПи»). Безусловно, кредитно-финансовые учреждения предпочитали использовать уже имеющееся оборудование, чтобы не нести лишних затрат и не совершать дополнительных действий.

Таким образом, возникла проблема технологической несовместимости криптографических устройств других вендоров с криптооборудованием, предлагаемым государственным заказчиком для подключения к СМЭВ.

Сложившаяся ситуация противоречила положениям постановления Правительства РФ от 22.12.2012 № 1382[1], согласно которым подключение к СМЭВ возможно, если используемые средства криптографической защиты информации (далее – СКЗИ) соответствуют требованиям, обеспечивающим технологическую совместимость информационных систем присоединяемой организации с инфраструктурой взаимодействия. Для решения проблемы технологической совместимости Минкомсвязи совместно с компанией «Ростелеком» и ведущими производителями криптографического оборудования организовали проведение конкурентного тестирования СКЗИ различных производителей, в том числе «С-Терра СиЭсПи», а затем создали пилотную зону на СКЗИ, альтернативных уже использовавшимся в СМЭВ средствам единственного производителя.

По результатам тестирования и испытаний в рамках пилотной зоны шлюзы безопасности С-Терра теперь внесены в перечень рекомендованного криптооборудования для подключения к СМЭВ. В федеральном центре обработки данных СМЭВ, на площадке «Ростелекома» уже установлены криптошлюзы компании «С-Терра СиЭсПи».

Таким образом, для целого ряда государственных, банковских структур и других финансово-кредитных организаций, использующих для обеспечения безопасности передаваемой информации шлюзы безопасности С-Терра, теперь созданы условия «наибольшего благоприятствования» при взаимодействии со СМЭВ.

Выбор оборудования

Требования к защите передаваемой информации при подключении к СМЭВ очень конкретны: безопасность должна обеспечиваться с помощью СКЗИ, сертифицированных по классу не ниже КС3[2], на основе межсетевого протокола IPsec, являющегося стандартом безопасности[3].

В опубликованном на технологическом портале электронного правительства обновленном

[1] Постановление Правительства РФ от 22.12.2012 № 1382 «О присоединении Информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (в ред. постановлений Правительства РФ от 22.11.2013 № 1056, от 21.07.2014 № 680).

[2] Пункт 118 «Технических требований…», утвержденных приказом Минсвязи России от 23.06.2015 № 210.

[3] Пункт 48.4 «Технических требований…», утвержденных приказом Минсвязи России от 23.06.2015 № 210.

Приложении 3 к «Регламенту обеспечения предоставления государственных услуг и исполнения государственных функций в электронном виде»[1] перечислены требования к сети передачи данных участников информационного обмена, в том числе с **рекомендациями по выбору оборудования компании «С-Терра СиЭсПи».**

Выбор подходящих шлюзов безопасности зависит от пропускной способности сети, количества автоматизированных рабочих мест (АРМ), их схемы подключения.

Таким образом, сотрудничество государства в лице Минкомсвязи России, технологического оператора ПАО «Ростелеком» и бизнес-сообщества позволило расширить список рекомендованного криптооборудования для подключения к СМЭВ. Особенно важно, что выбор оборудования для включения в этот перечень проходил на основе свободной конкуренции между участниками рынка средств обеспечения информационной безопасности.

Участники СМЭВ получили эффективный способ подбора необходимого технологического оборудования для дальнейшей реализации важной государственной программы. При этом приобретен положительный опыт сотрудничества с мощным синергетическим эффектом, который в дальнейшем, надеемся, будет использован в других государственных программах, предполагающих применение высокотехнологичного оборудования.

[1] Регламент 3.4, Приложение 3 «Требования к сети передачи данных участников информационного обмена» (http://smev.gosuslugi.ru/portal/api/files/get/80937).