СМЭВ ДЛЯ БАНКОВ: ПОДКЛЮЧАЕМСЯ БЕЗОПАСНО

Мария ЛУРЬЕ,
руководитель отдела маркетинга ООО «С-Терра СиЭсПи»

ЧТО ТАКОЕ СМЭВ

Сегодня уже мало кому нужно объяснять, что такое СМЭВ. Эти магические четыре буквы, которые еще пять лет назад вызывали недоумение, расшифровываются сразу и легко — Система межведомственного электронного взаимодействия. Она есть Единая (тогда букв становится пять), есть территориальная, но в любом случае подразумевает электронное взаимодействие государственных и муниципальных органов как между собой, так и с другими организациями. И всё это для облегчения жизни нам, гражданам России.

ЗАЧЕМ ОНА БАНКАМ

Финансовые организации не остались в стороне и тоже присоединились к единой системе. В качестве пользователей и поставщиков информации. И если получение сведений от органов государственной власти посредством СМЭВ — дело добровольное (многие признают, что это удобно и быстро), то передача данных о платежах в пользу бюджета в систему ГИС ГМП (Государственная информационная система о государственных и муниципальных платежах)– это обязанность, зафиксированная в Федеральном законе РФ № 210-ФЗ от 27.07.2010[1]. Уже действует жесткое правило, что банки, не подключенные к ГИС ГМП, не могут принимать платежи в бюджет.

Поскольку координатором организации взаимодействия с банками и оператором ГИС ГМП является Федеральное казначейство, то финансовым организациям необходимо вначале пройти там регистрацию в качестве участников системы, а потом подключиться к СМЭВ.

Мы уже выяснили, что подключение банков к СМЭВ — процедура обязательная. Теперь уточним, что это взаимодействие должно быть еще и защищенным. **Организация защищенного канала связи — необходимое условие подключения к СМЭВ.** Разберемся с этим подробнее.

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

Начнем с технических требований. Они установлены Приказами Минкомсвязи России № 210 от 23.06.2015, № 120 от 3 мая 2014 г. и № 390 от 9 декабря 2013 г. Последние перечисленные приказы относятся к организациям, которые не участвуют в предоставлении или организации предоставления государственных и муниципальных услуг, но подключаются к СМЭВ. На банки их действие тоже распространяется.

Для удобства представим одним списком требования из перечисленных приказов, которые должны выполнять финансовые организации, подключаясь к СМЭВ. Они заключаются в следующем:

1. Для обеспечения сетевой защиты данных должен использоваться набор протоколов IPsec

2. СКЗИ должны быть сертифицированы ФСБ России по классу КС3

3. Межсетевой экран должен быть сертифицирован ФСБ России по 4 классу (МЭ4) и ФСТЭК России по 3 классу (МЭ3)

4. Обязательно резервирование каналов связи

Кроме этого, в Приложении 4[2] к регламенту определено требование использования СКЗИ рекомендованных вендоров. Отмечу, что **всем пунктам требований отвечают только шлюзы безопасности С-Терра**. Они сертифицированы ФСБ России, в том числе по классу КС3, работают по протоколам IPsec, выполняя требования ГОСТ, содержат интегрированный сертифицированный обоими регуляторами межсетевой экран.

РЕКОМЕНДАЦИИ ОТ «С-ТЕРРА СИЭСПИ»

Когда речь заходит про СМЭВ, оказывается, что «все ходы записаны» и «всё запротоколировано» — остаётся только выполнять. Собственно, это мы и предлагаем сделать. Нагляднее всего рекомендации[2] по выбору криптооборудования С-Терра для защищенного подключения к СМЭВ представить в виде простой таблицы *(Таблица 1)*.

Хочу обратить внимание на то, что можно выбрать как супермощный и высокопроизводительный шлюз, который, конечно, будет стоить соответственно, так и компактное и недорогое устройство. Для каждой позиции доступен большой выбор аппаратных платформ, на которых СКЗИ может быть установлено. Более того, так как желания и комфорт пользователей для нас приоритетны, мы готовы протестировать любую предоставленную партнером или заказчиком аппаратную платформу и, при благоприятном результате тестов, установить на нее СКЗИ С-Терра Шлюз.

Таблица 1. Рекомендации по выбору криптооборудования С-Терра для защищенного подключения к СМЭВ

Продукт С-Терра	Количество серверов, АРМ и терминалов в защищаемом сегменте	Необходимая производительность шифрования
С-Терра Шлюз 7000	более 300	до 2,7 Гбит/с
С-Терра Шлюз 3000	от 100 до 300	до 300 Мбит/с
С-Терра Шлюз 1000V	от 50 до 100	до 100 Мбит/с
С-Терра Шлюз 100V	от 5 до 50	до 15 Мбит/с
С-Терра Шлюз 100	от 3 до 5	до 15 Мбит/с
С-Терра Шлюз 100B	от 1 до 2	до 15 Мбит/с

Остается определиться с тем, с какого количества рабочих мест будет организован доступ в систему, какой объем данных будет циркулировать по защищенным каналам связи — и вперёд, за шлюзами безопасности к нам, в «С-Терра СиЭсПи», к любому из наших партнеров или непосредственно в «Ростелеком».

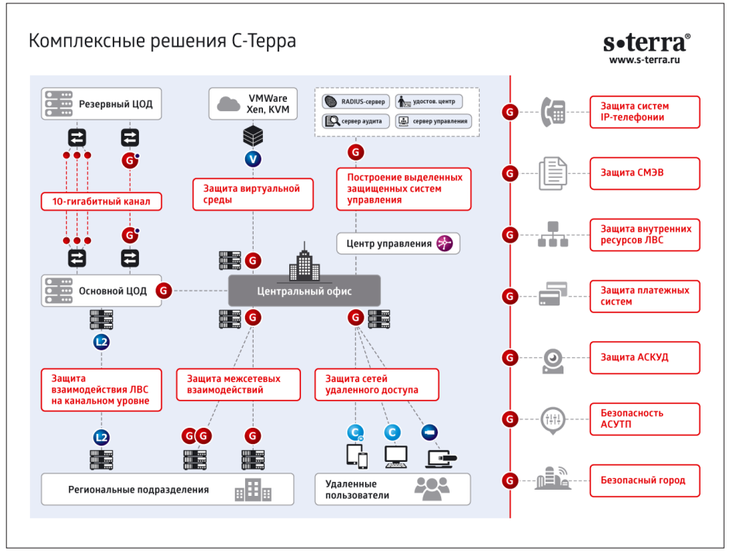
В федеральном ЦОД СМЭВ — на площадке «Ростелеком» — шлюзы С-Терра установлены, успешно защищают каналы связи при взаимодействии организаций с системой и ждут новых подключений.

Организации подключаются к СМЭВ за счет собственных средств. А банкиры умеют считать деньги — профессия такая. Поэтому стоит продумать оптимальную схему подключения, позаботиться о горячем резервировании, выбрать криптошлюз того производителя, оборудование которого уже обеспечивает безопасность информационной системы банка, — всё это позволит эффективно расходовать средства и даже сэкономить на обслуживании в будущем. Если же в вашем банке для защиты каналов связи используются не шлюзы С-Терра, то алгоритм действий не меняется: выбираете С-Терра Шлюз — приобретаете — устанавливаете. И это тоже прописано в Приложении 4 к Регламенту: «…если в подключаемой организации используются СКЗИ другого производителя, следует обеспечивать перешифрование трафика…» на СКЗИ вендора, прописанного в Требованиях[2]. Перефразируя старинную поговорку, все пути ведут в С-Терра.

ЧТО ЛУЧШЕ, 3 ИЛИ 2?

Переход к СМЭВ 3.0 в самом разгаре. Новая версия системы более функциональна, технологична и удобна. В отличие от СМЭВ 2.0, она предполагает взаимодействие между органами власти субъектов РФ, а не только между регионом и федеральным центром. Это стало возможно вследствие упрощения топологии системы, организации прямой доставки запросов от одного участника взаимодействия к другому.

С точки зрения обеспечения безопасности ничего не меняется. Использование шлюзов безопасности С-Терра для защищенного подключения к СМЭВ рекомендовано Минкомсвязью, удовлетворяет всем требованиям, и кроме того, позволит вам эффективно распорядиться выделенным на эти цели бюджетом и разумно организовать дальнейшую работу своей информационной системы во взаимодействии с СМЭВ.



[1] Федеральный закон от 27.07.2010 № 210-ФЗ (ред. от 28.07.2012)»Об организации предоставления государственных и муниципальных услуг». С 01.01.2013 года все кредитные организации при осуществлении платежей, являющихся источниками формирования доходов бюджетов бюджетной системы РФ (пошлины, штрафы, налоги юридических и физических лиц), обязаны незамедлительно направлять информацию о фактах оплаты в систему — в связи с вступлением в силу требований статьи 21.3 Федерального закона и вводом в эксплуатацию ГИС ГМП Федерального казначейства

[2] Смотри Приложение 4 «Требования к сети передачи данных участников информационного обмена» Регламента обеспечения предоставления государственных услуг и исполнения государственных функций в электронном виде (Технологический портал СМЭВ *https://smev3.gosuslugi.ru/portal/*)