

Российский рынок СКЗИ



Международная конференция «РусКрипто» стала авторитетной площадкой для общения специалистов в области криптографии и защиты информации, обсуждения актуальных проблем и поиска их решений. В конференции традиционно принимают участие разработчики и пользователи криптографических шифровальных средств, представители науки, регуляторных структур, государственных и коммерческих предприятий. Аудитория конференции – около 250 человек. География участников постоянно расширяется как по России (Москва, Санкт-Петербург, Новосибирск, Ростов на Дону, Курск, Самара, Пермь, Воронеж и т. д.), так и по СНГ (Россия, Белоруссия, Азербайджан, Армения, Казахстан, Украина) и странам дальнего зарубежья (США, Китай, Чехия, Германия).

С каждым годом программа конференции становится более насыщенной. Тринадцатая конференция «РусКрипто'2011» не стала исключением. В ходе конференции прошли секции, посвященные направлениям развития криптографии, теории и практике криптографии и криптоанализа, информационной безопасности в Интернете, вопросам преподавания криптографических дисциплин в высшей школе, академическим исследованиям в сфере информационной безопасности, использованию криптографии при оказании государственных услуг в электронном виде.

Одним из событий прошедшей конференции стал круглый стол «Российский рынок СКЗИ». Предлагаем вниманию читателей некоторые факты и мнения, озвученные в ходе состоявшейся дискуссии.

Проблема выбора, или Товар лицом

Тон обсуждению задал Сергей Кирюшкин, советник генерального директора ООО «Газинформсервис». Он обратил внимание аудитории на проблему, с которой сталкиваются как потребители СКЗИ, так и интеграторы, которым поручается реализация проекта, – это проблема полноты информации о

продуктах, предлагаемых производителями. Основным источником такой информации служат сайты производителей. Участникам круглого стола был представлен в виде таблицы результат сравнительного анализа информации, важной для обоснования выбора производителя, представленной на сайтах ряда ведущих российских производителей СКЗИ.

Наличие сертификата, функции, области применения, совместимость с платформами и интерфейсами, рекомендуемые ключевые носители, реализуемые алгоритмы, наиболее распространенные совместимые приложения – это то, что указано на сайтах практически всех производителей. В части доступных комплектов документации начинаются расхождения. В лучшем случае на интернет-витрине можно найти инструкцию по эксплуатации, инструкцию администратора, формуляр. Более детальные описания, как правило, нужно запрашивать дополнительно. Между тем каждый запрос и ожидание ответа – это лишняя нагрузка на бюджет проекта. Не всякий интегратор пойдет на то, чтобы делать серию запросов для детализации выборки.

В некоторых случаях производитель заявляет о возможности бесплатного получения СКЗИ с его сайта, в частности для реализации

госуслуг. Некоторые предлагают демо-версии, а кое-кто – даже бесплатное скачивание полнофункциональной версии СКЗИ, указывая согласованный с регулятором способ упрощенного распространения СКЗИ.

Публикация характеристик надежности и производительности – пока редкое исключение. Хотя такая информация очень актуальна, поскольку в проекте, как правило, существует условие, чтобы средства защиты информации не уменьшали существенно показателей надежности и производительности системы в целом.

Раздел «особенности применения» был обнаружен у одного производителя, однако в этом разделе были представлены и вопросы совместимости, и реализованные криптографические алгоритмы, и многие другие аспекты. Это говорит о том, что информация не систематизирована.

Указание совместимости с другими СКЗИ – несомненный признак заботы вендора о потребителе. Но такая информация представлена не у всех.

Вывод, который сделал докладчик, таков: крайне желательно наличие единого шаблона, согласно которому лицензиаты ФСБ представляли бы «на витрине» информацию о своей продукции. Интегратору, как коммерческой структуре,

Параметры	Производители	1	2	3	4	5
Сертификат			+	+	+	+
Функции		+	+	+	+	+
Области применения		+	+	+	+	
Совместимость (платформы и интерфейсы)		+	+	+	+	+
Алгоритмы		+	+	+	+	+
Ключевые носители		+	+	+	+	
Совместимые приложения		+	+	+	+	+
Документация		+	+	+		
Загрузить демо-версию		+	+		+	
Загрузить полнофункциональную версию				+		
Характеристики надежности			+			
Характеристики производительности			+			+
Особенности				+		
Совместимость с другими СКЗИ и в какой части					+	+
Цена		+	+	+	+	+

не всегда может быть выгодно самостоятельно проводить полный анализ возможностей имеющихся на рынке СКЗИ, кроме того, в ходе такой работы он наверняка будет соблюдать свои интересы. Вероятно, в результате проекта потребитель получит решение, на данный момент достаточно эффективное. Но появляются новые версии ОС, патчи, новые ключевые носители, новые приложения, новые задачи, угрозы, и представить себе аналитический отдел, который будет постоянно отслеживать всю эту сложную динамическую картину, довольно сложно. Получит ли потребитель в этих условиях вовремя обновляемое и качественно сопровождаемое решение? Наличие единых требований регулятора к тому, как лицензиаты должны представлять на рынке свою продукцию, позволило бы потребителям получать более гармоничный продукт.

Александр Баранов, первый заместитель начальника Центра ФСБ России, частично поддержал г-на Киришину: «Зачастую из сайтов производителей невозможно понять, в чем состоит реальное отличие продукта. На рынке присутствуют десятки три IP-шифраторов разных производителей. В чем отличие одного от другого, каковы преимущества того или иного решения, узнать крайне сложно». Сертификаты ФСБ – унифицированные.

Института независимых экспертов, хотя бы в области потребительских качеств СКЗИ, нет. Конечно, инструментальная часть подобной экспертизы (организация стенда, например для исследования характеристик пропускной способности) довольно сложна, трудоемка, требует привлечения высококвалифицированных специалистов и стоит приличных денег. Но без объективной картины пользователь не может ориентироваться на рынке.

Что касается возможностей регулятора, то, как указал Александр Баранов, они довольно сильно ограничены, регулятор не может «делать все». «Возникает вопрос, где создавать базу для проведения анализа аппаратуры? Для этого, видимо, нужна некая общественная организация, причем она должна обладать солидными средствами», – считает г-н Баранов.

«АЗИ (Ассоциация защиты информации) – организация, в которую входят многие производители. Это площадка, на базе которой и можно проводить оценку СКЗИ, – считает Александр Соколов, председатель совета директоров ЗАО «Лаборатория СКАТ». – Возлагать такую обязанность на регулятора нельзя. Это должна быть общественная организация, состоящая из профессионалов». Участие производителя в проекте по независимой оценке СКЗИ – показатель

того, что его продукт действительно конкурентоспособен, а участие в проекте многих конкурирующих производителей даст в итоге объективную картину.

Юрий Маслов, коммерческий директор компании «КРИПТО-ПРО», напомнил, что помимо интеграторов, есть еще разработчики прикладных систем, в которые встраиваются шифровальные криптографические средства. Поэтому если речь идет о том, чтобы давать более полную информацию о предлагаемых СКЗИ, то нужна также информация том, как правильно применять шифровальные криптографические средства в прикладных системах. Коль скоро нет обязательных нормативных документов в этой области, имеет смысл создать документы, принятые профессиональным сообществом, подобные RFC (информационным документам Интернета, содержащим технические спецификации и стандарты, применяемые во Всемирной сети). Такой документ, обсужденный сообществом и одобренный регуляторами, получит моральный статус, и на соответствие этому документу сможет проводиться экспертиза СКЗИ. Такая экспертиза, пусть и добровольная, поможет урегулировать тот хаос в применении шифровальных криптографических средств, который имеет место сейчас.

Рынок СКЗИ и ВТО

Возможное вступление России в ВТО откроет путь на рынок зарубежным производителям СКЗИ. Как СКЗИ будут проверяться? Сохранится ли национальная система требований к шифровальным криптографическим средствам? Этот вопрос также поставил Юрий Маслов.

Слово взял Александр Баранов: «Все знают, что лицензия на разработку шифросредств невозможно получить, не имея лицензии ФСБ на работу с гостайной. Существующие требования содержат закрытую часть. Потому что их открытая публикация фактически означала бы раскрытие в значительной степени методов, которые используются для получения государственной важной информации путем дешифрования».

Но ряд методов, которые раньше считались секретными, сейчас опубликованы (например, метод Мацуи), развивается открытая криптография. И ФСБ это учитывает. В частности, требования к шифровальным средствам для защиты систем персональных данных несекретны и опубликованы. «Думаю, в этом направлении можно будет поработать, по крайней мере для нижних классов нарушителей (Н1–Н3)», – сказал представитель ФСБ.

Однако ФСБ регулирует не все: «Корпоративные сети вообще нами не регулируются, в них возможно применение любых СКЗИ, если только сети не используются для оказания услуг сторонним клиентам». Поэтому в корпоративных сетях используется «все, что угодно». Примеры – сети банкоматов, где используется TripleDES, система SWIFT, которая работает на оригинальной криптосхеме, и ряд других систем, которые в силу отсутствия отечественных аналогов работают с импортной криптографией. «Но в тех отраслях, в которых требуются сертифицированные СКЗИ, сертификация будет требоваться и для импортных средств. И если зарубежные производители не пойдут на раскрытие соответствующих деталей и проведение сертификационных испытаний, их тут не будет», – резюмировал Александр Баранов.

Долгое время регуляторы держали рынок отечественной криптографии

«в тепличных условиях». Смогут ли российские производители со вступлением страны в ВТО быть конкурентоспособными? Как считают многие участники дискуссии, смогут.

«Конечно, мы немножко потеряем, если сюда придут крупные мировые компании. У них больше рынки, и на этих рынках они работают дольше, чем мы. Но, к счастью, рынок СКЗИ за последние годы сильно вырос, и те отечественные компании, которые делают качественную продукцию, даже в мировом масштабе являются значимыми. По некоторым продуктам наши разработчики СКЗИ могут неплохо конкурировать», – убежден Дмитрий Горелов, коммерческий директор компании «Актив».

«В стране создано сообщество, которое невелико в масштабе экономики, но которое объединяет сотни компаний-лицензиатов, выпускает сотни наименований продуктов и создает продукцию, которая вполне способна конкурировать на рынке», – отметил Сергей Рябко, президент группы компаний «С-Терра». В «лобовой» конкуренции с ведущими мировыми вендорами отечественным производителям, конечно, не выиграть – в силу масштабов их бизнеса, объемов средств, которые они способны вложить в маркетинг, исследования, систему сбыта. Но можно, например, «ставить точки контроля в те критические места оборудования, которые вызывают сомнения. Предположим в оборудовании зарубежного производителя есть «закладка». Закладка его в свой туннель, который не пропускает наружу лишнего трафика. Не обязательно обладать всей мощью технологий именитого вендора, чтобы «держать его в рамках», – отметил Сергей Рябко. Целесообразно также стимулировать зарубежных производителей к открытию локального производства.

Василий Долматов, заместитель генерального директора ООО «Криптоком», высказал следующее мнение: «В отношении тех продуктов, которые придут на рынок после вступления России в ВТО, у потребителя должно быть четкое понимание, где и что он может использовать, а где и что использовать не надо. Это позволит некоторым образом разграничить сегменты рынка. А для производителя очень важно уметь конкурировать с зарубежными

вендорами на их поле. У нас сейчас очень скромный опыт создания продуктов, конкурирующих с их продукцией по функционалу». Но даже если продукт российского производства обладает достойным функционалом, его преимущества придется как-то доказывать. Таким образом был вновь поднят вопрос объективного сравнения рабочих характеристик различных продуктов.

Вопрос о «конкуренции на их поле» прокомментировал Александр Баранов. В Европе не запрещено продвигать криптосредства на рынке другой страны. Но не получается. «Применение СКЗИ в госорганах регулируется дополнительными инструкциями. Государственные организации их соблюдают и отдают преимущество национальным средствам. В первую очередь это касается закрытых систем, но также и систем, обрабатывающих конфиденциальную информацию. Нужно изучать зарубежный опыт, чтобы предлагать пути решения этого вопроса. И если подобные предложения исходят от общественных организаций, на основании анализа опыта «снизу», отношение к предложениям «сверху» совсем другое».

Но опять же анализ зарубежного опыта, так же как и проведение независимой экспертизы криптосредств, требует вложений и усилий. Очевидно, что без совместной работы представителей бизнеса в рамках СРО или иной общественной организации, например АЗИ, здесь не обойтись.

В заключение хотелось бы поблагодарить организаторов – Ассоциацию «РусКрипто» и Академию информационных систем – за радужный прием, содержательную программу мероприятия, включившую помимо непосредственно конференционной части также соревнование студенческих команд «РусКрипто STF'2011». Усилия организаторов позволили «РусКрипто» стать по-настоящему авторитетным и масштабным ежегодным форумом для обмена опытом и обсуждения насущных отраслевых проблем специалистами в области криптографии и защиты информации. Надеемся, что в следующем году мы снова сможем порадовать наших читателей интересными материалами с очередной конференции «РусКрипто». ■