NBJ: Очередное заседание нашего круглого стола посвящено анализу вопросов и проблем, возникающих в рамках обеспечения информационной безопасности в банках. Хотели бы сразу отметить, что эту тему мы поднимаем регулярно, не реже двух раз в год. И сейчас мы не видим причин отступать от традиции, поскольку количество рисков в сфере ИБ возросло, проблем у финансово-кредитных организаций с защитой информации наверняка прибавилось.

С учетом этого первый вопрос мы хотим сформулировать следующим образом: как участники круглого стола, представители банков и компаний-разработчиков, видят основные вызовы в сфере ИБ в настоящее время?

Р. ХАРИТОНОВ: «С-Терра СиЭсПи» давно работает с банками, поэтому мы можем поделиться своими наблюдениями. Ни для кого не секрет, что бюджеты, отведенные под развитие ИБ, стараются урезать или оставить без изменений. Так что априори понятно – кредитные организации будут приобретать меньше инструментов ИБ, чем раньше.

В этой связи я хотел бы расширить вопрос модератора: какие выходы для себя из сложившейся ситуации видят банки, на что они готовы пойти ради экономии средств? Поменялись ли взгляды банкиров на такой инструмент, как виртуализация, поскольку, с нашей точки зрения, ее использование – это возможность оптимизировать затраты финансово-кредитных организаций?

В. ОКУЛЕССКИЙ: На мой взгляд, вопрос сформулирован некорректно. И посыл в результате тоже получается непра-

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

Импортозамещение – одна из самых популярных сегодня тем для обсуждения. В России вводится национальная платежная система, создаются новые ЦОД для хранения данных, в то же время участились сообщения информационных агентств о более масштабных киберпреступлениях. В этих условиях необходимо обеспечить надежную и легитимную с точки зрения российских стандартов защиту данных не только в местах их хранения и обработки, но и в процессе их передачи. То есть без построения виртуальных частных сетей (VPN) не обойтись.

Не секрет, что в банковских информационных системах предпочитают использовать западные средства безопасности. Можно говорить о том, что западные VPN-продукты обладают большей функциональностью, и работа с ними привычнее и удобнее. Но привычка – дело времени, а времена меняются, требуя иных подходов. Наступает период, когда и финансово-кредитные организации задумываются о том, как удобнее заменить западные алгоритмы защиты каналов связи на российские.

К тому же перечень отечественных средств безопасности с каждым днем становится шире, растет удобство использования и качество обслуживания. Не стоит забывать и о том, что российские производители готовы гибко и оперативно реагировать на потребности заказчика, создавая специализированные решения для конкретных проектов. Кроме того, их продукция отвечает всем требованиям российского законодательства, в частности СТО БР ИББС, согласно которому рекомендуется применять VPN-продукты, сертифицированные ФСБ России.

Инфраструктура банковской информационной сети, как правило, диктует использование разнообразных решений по защите данных. Необходимо обеспечить безопасность информации не только внутри сети организации, но и при взаимодействии с отдаленными филиалами, с ЦОД, с мобильными пользователями, с банкоматами и даже с зарубежными представительствами. Все эти задачи полноценно решаются с применением продуктов российских вендоров. В частности, надежную комплексную систему защиты каналов передачи данных в банковских информационных системах обеспечивают средства безопасности «С-Терра».

Закономерным результатом развития рынка в современных экономических условиях стало появление виртуального криптошлюза, который интегрируется непосредственно в виртуальную инфраструктуру. Благодаря его использованию, существенно экономится электроэнергия, место в стойке, снижаются затраты на обслуживание и техническую поддержку. Например, продукт «С-Терра Виртуальный шлюз» имеет минимальные сроки поставки и привлекательную стоимость. Это единственный на текущий момент виртуальный VPN-шлюз, сертифицированный ФСБ России и ФСТЭК России. Являясь, по сути, программным комплексом, он обладает полноценной функциональностью шлюза безопасности на аппаратной платформе, а возможность его установки на одну аппаратную платформу совместно с другими программными средствами (системы обнаружения и предотвращения вторжений, антивирусные программы, почтовый сервис, CRM и пр.) обеспечивает надежную эшелонированную защиту и удобство использования.

Основой повышения безопасности банковского взаимодействия является использование надежных, проверенных временем и регуляторами, соответствующих российским стандартам инструментов защиты, которые при этом обеспечивают оптимальное соотношение удобства, свободы пользователя, степени защиты и понесенных затрат. Не стоит забывать при этом о стремительном развитии технологий, растущем многообразии угроз, увеличивающейся глубине виртуализации информационного пространства, а также о национальной безопасности.