# Особенности сетевой безопасности в банках

***Обзор решений для сетевой информационной безопасности для банковских структур в контексте требований, предъявляемых к подобным системам стандартом СТО Банка России.***

**Руслан Нигматулин –** директор департамента по работе с корпоративными клиентами ЗАО "С-Терра СиЭсПи".

## *Введение*

*Информационная безопасность в финансовой индустрии – это обширная тема с очень разнородной спецификой. Не претендуя на полноту анализа в небольшой статье, хотелось бы рассказать о некоторых наблюдениях по итогам ушедшего года. Наблюдения в данном случае будут с "колокольни" компании – разработчика решений VPN и СКЗИ. Уже который новый год оборудование компании "С-Терра" в полной "боевой" готовности встречает трафик в сетях передачи данных. Встречает, шифрует и провожает. Пожалуй, это тот случай, когда праздничные сюрпризы не к месту. Все должно быть предсказуемо и предельно стабильно. К концу 2012 г. уже около двухсот банков используют продукты S-terra для защиты своих сетей, в соответствии с требованиями российского законодательства. Среди них немало банков из первых десятков финансового рейтинга.*

## Что принес 2012 год?

Что можно сказать, посмотрев на события прошедшего года? Индустрия информационной безопасности – одна из самых консервативных и не приемлет инноваций без тщательной апробации. В 2012 г. российские банки продолжили совершенствовать свои сети под "зорким взглядом" регуляторов. Все большее количество банков присоединяются к стандарту СТО БР, играющему важную роль в регулировании ИБ в системе. В стандарте четко обозначена мысль о национальной, государственной значимости банковской системы. И, соответственно, обеспечение необходимого уровня информационной безопасности является важнейшим условием развития и укрепления банковской системы Российской Федерации. Когда речь идет о государственных интересах, сразу же встает вопрос о необходимости собственных технологических разработок, с одной стороны, и об использовании мировых достижений, с другой. И здесь криптографическая наука, как один из показателей технологической развитости страны, уже давно встала в один ряд с другими стратегическими составляющими. И вполне естественно, что использование средств криптографической защиты информации выделено отдельным и весьма важным пунктом в документе стандарта Банка России. Стандарт без двусмысленностей и размытости четко обозначает требования к СКЗИ, такие как: определенный класс защиты, документированность, реализация процедур мониторинга и др. Использование международных сетевых стандартов, с одной стороны, и соответствие требованиям национальных регуляторов, с другой, – данный подход, выбранный компанией "С-Терра", на практике доказал свою востребованность. Решения для построения VPN, соответствующие требованиям RFC, работающие на российских криптоалгоритмах и сертифицированные в органах технического регулирования (ФСБ России, ФСТЭК России), хорошо "прижились" в коммерческих структурах, которые весьма требовательны к соотношению цена–качество.

По современным темпам развития, можно сказать, в далеком 2006 г. впервые на аппаратной платформе Cisco Systems выпущен продукт NME-RVPN для российского рынка. Компания "С-Терра", как официальный технологический партнер Cisco Systems в статусе Solution Technology Integrator, обеспечила производство в России продуктов NME-RVPN. Сейчас продукт NME-RVPN уже в новой модификации, как модуль MCM, продолжает успешно внедряться и эксплуатироваться. Приоритетная реализация национальных стандартов с использованием лучших западных технологий стала одной из основ бизнес-стратегии компании. Этот принцип как нельзя более актуален для финансовой сферы. Банки не могут изолированно существовать в отдельно взятой среде одного государства, не могут и не должны использовать кустарные продукты. Особенно в период бурного роста, когда важно использовать надежные, проверенные технологии.

Развитие филиальных сетей банков стало одной из самых заметных тенденций в 2012 г. Вместе с количеством банковских офисов росло и количество банкоматов, и количество сотрудников, и количество клиентов банков. Развитие ИБ привязано к развитию собственно банковской системы. Соответственно, выросло количество используемых шлюзов безопасности и программных клиентов, защищающих рабочие места. Единая сеть, состоящая из более чем тысячи защищенных элементов, уже не является чем-то диковинным. Очень важно при интеграции решений ИБ в сеть, где применяется огромное количество другого разнородного оборудования, избежать лишнего реинжиниринга, переделки архитектуры. А это возможно только тогда, когда оборудование ИБ изначально разрабатывалось в едином ключе со всем остальным сетевым семейством. Шлюзы безопасности S-terra, обеспечивающие защиту данных на основе набора протоколов IPsec, разрабатываются именно по такому принципу. Набор протоколов IPsec дает все преимущества стандартного дизайна: гибкость архитектуры, многолетний и массовый экспертный анализ, исчерпывающую документированность поведения продукта, кросс-отладку с любым независимым третьим производителем.

При росте и разветвлении защищаемой сети, кроме усложнения структуры, наблюдается и рост трафика, в первую очередь, в центральных узловых точках. Вспомним, что шифрование и контроль целостности – ресурсоемкие операции, при неправильном построении системы передачи данных именно они становятся узким местом. Чтобы не создавать проблем в работе ИТ-сервисов, следует уже на этапе проектирования учитывать про-

изводительность шифрующих средств. Ресурсы шлюза безопасности тратятся приблизительно в равной степени на шифрование и на дешифрование трафика.

Еще один фактор, влияющий на производительность, – профиль трафика, или, проще говоря, частота встречаемости пакетов разной длины. Производительность – комплексная величина, зависящая от множества факторов. Для сетевых устройств безопасности она будет включать в себя как сетевую производительность, так и производительность шифрования. Для компаний-разработчиков своевременный выпуск решений для растущего трафика – всегда актуальная задача. В 2012 г. компания "С-Терра" вместе с Cisco представили совместную разработку – высокопроизводительное решение для защиты канала с агрегированной производительностью шифрования 10 Гбит/с. Данное решение необходимо, в частности, там, где для хранения и обработки больших объемов конфиденциальной информации используются распределенные центры обработки данных (ЦОД). С его появлением стало проще и дешевле как защищать передаваемую информацию между ЦОДами, так и обеспечивать высокую производительность для доступа пользователей к ресурсам ЦОД. Кроме того, такое высокопроизводительное шифрование потока данных может применяться в облачных технологиях, а также при миграции сетевой инфраструктуры, особенно, если речь идет о больших финансовых структурах. Достичь высокой производительности позволили такие факторы как: мощная аппаратная база, скоростные интерфейсы, оптимизированное ПО.

Другая тенденция, если не появившаяся, то точно усилившаяся в 2012 г. – интерес к мобильным решениям ИБ. Здесь, надо признать, собственно инициатива пришла не из сферы ИБ, а от бизнеса, что, в общем-то, правильно. Потрудиться над поиском решений пришлось всем: и компаниям-разработчикам, и подразделениям ИБ-организаций, и регуляторам. Отечественные трудности мобильной ИБ можно разделить на две основные составляющие: нормативно-техническую и коммерческо-техническую. Нормативные трудности – это такие, как, например, запрет регулятором работы СКЗИ при включенном штатном выходе в радиоканал, необходимость фиксирования ОС и др. Коммерческие и технические трудности – необходимость разработки ПО под различные ОС, различные платформы, производители которых не всегда открывают доступ для встраивания национальных решений ИБ. Все это привело к тому, что появились довольно странные и для специалистов ИБ, и для потребителей решения, такие как защищенный доступ при условии jailbreak (по сути, взлом операционной системы) или планшетный компьютер, на котором нельзя обновить ОС. В банковских и финансовых структурах оперативность бизнеса, как залог конкурентоспособности, очень важна, и, конечно, мобильные защищенные решения здесь востребованы. Причем, как для корпоративного применения сотрудниками, так и для предлагаемых услуг клиентам. Но банк никогда не предложит клиенту сделать jailbreak на новом iPhone, да при этом еще и установить устаревшую версию ОС. Да и для внутрикорпоративного применения такой вариант маловероятен. Только легитимное и с точки зрения регулятора, и с точки зрения производителя решение может быть честно предложено пользователю. Компания "С-Терра" при разработке мобильных решений внимательно учитывает требования пользователей. На конференции Cisco Expo 2012 были представлены планшет и смартфон Samsung с установленным клиентом безопасности S-terra и пакетом приложений Cisco для мобильных устройств. Они вызвали ожидаемо высокий интерес среди посетителей.

Такие принципы как технологичность, стандартизация и совместимость, унификация получили развитие и в других составляющих продуктовой линейки компании "С-Терра". Эти принципы можно рассмотреть на следующем примере.
В 2012 г. обновилась система управления продуктами безопасности S-terra: на смену продукту VPN Updater пришла новая версия системы централизованного управления "С-Терра КП". Основное назначение "С-Терра КП" – повышение общего уровня контроля за VPN-сетью, предоставление удобных средств развертывания и последующее управление VPN-устройствами. Продукт адресован администраторам средних и крупных сетей и является базовым инструментом для удобной и эффективной эксплуатации VPN-сетей, строящихся на основе продуктов компании "С-Терра". В соответствии с принципами построения сетевой инфраструктуры, система управления должна выполнять строго свои функции и быть полезным, но не навязанным элементом. То есть, устранение системы управления никак не скажется на непосредственном функционировании сети. Этот, казалось бы, очевидный принцип не всегда соблюдается отечественными разработчиками. Часто российские софтверные компании придумывают собственный велосипед (наступая при этом на грабли), давно изобретенный другими. Система управления "С-Терра КП" выполняет функции в строгом соответствии с сетевой логикой и архитектурой. Устанавливая продукт "С-Терра КП", пользователь получает доступ к удобным и современным методам управления. Очевидный вывод: в небольших сетях, например, до десятка узлов, которые недалеко разбросаны географически и легко доступны, можно не использовать систему управления, и, соответственно, сэкономить деньги. Другой очевидный вывод: независимость работоспособности узлов защищенной сети – шлюзов безопасности – от системы управления, позволяет рассматривать последнюю как менее критичный элемент. Для практикующего администратора, инженера-эксплуатационщика немаловажно то, что в сети становится одним критичным элементом меньше. В итоге, система управления занимается тем, чем и должна: задание настроек, мониторинг, инвентаризация и т.д.

## *Заключение*

*В 2012 г. произошло важное изменение в законодательстве, касающееся ИБ – вышло Постановление Правительства РФ № 1119 от 01.11.2012 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Видимо, в 2013 г. нас ждет последовательный выход подзаконных актов, рекомендаций регуляторов и др. Так что будем ждать изменений.*

***Руслан Нигматулин,***
*компания ЗАО "С-Терра СиЭсПи"*