# Риски ДБО можно и нужно контролировать

## В. КОНЯВСКИЙ: «Невозможно обеспечить защищенность без создания доверенной среды, и невозможно обеспечить создание доверенной среды без аппаратных средств»

Беседовала: Софья Мороз

**В соответствии со вступившим в силу Законом «О национальной платежной системе» банки должны будут возмещать клиентам финансовые потери, понесенные в результате хакерских атак на системы ДБО. Готовы ли банки к этому, смогут ли они отказаться от старого принципа, гласящего что «спасение рук утопающих – дело рук самих утопающих»? На эти и другие вопросы отвечает в интервью НБЖ научный консультант ОКБ САПР Валерий Конявский.**

***НБЖ: Каков масштаб финансовых потерь и репутационных рисков для банков в связи с атаками на ДБО, по вашей оценке? В какой мере банки осознают значимость этих рисков?***

**В. КОНЯВСКИЙ:** Финансовые потери значительные, репутационные риски огромны. Однако пока финансовые потери зачастую удавалось компенсировать за счет клиентов. Теперь эта возможность значительно сузилась, и осознание масштаба потерь будет расти вместе с потерями. Репутационные же риски, в первую очередь, значимы для крупных клиентских банков с амбициозными планами. Мое ощущение – в целом банки осознают значимость рисков в сфере ДБО, но пока считают, что есть дела поважнее.

***НБЖ: Готовы ли банки к вступлению в силу нормы Закона «О национальной платежной системе», которая гласит, что банк должен сначала возместить клиенту деньги по его заявлению, а уже потом проводить расследование?***

**В. КОНЯВСКИЙ:** Нет. Пока состояние банков можно охарактеризовать как растерянность. Ясно, что все это не за горами, сейчас вот-вот появится множество исков, как справедливых, так и мошеннических, надежды на средства защиты нет, хакеры творят, что хотят. И что же делать?

Думаю, мы все должны сегодня банкам помочь. Причем помочь добросовестно, не стараясь, как это уже неоднократно замечалось за рядом вендоров, нажиться на имитации защиты. Решения есть, и их нужно быстро внедрять и популяризировать.

***НБЖ: Каков минимальный набор защиты при ДБО со стороны банка и со стороны клиента?***

**В. КОНЯВСКИЙ:** Со стороны банка должна быть создана настоящая, полнофункциональная доверенная среда. Как минимум, это «санитарная зона», комплекс средств периферийной защиты, сертифицированные средства СЗИ НСД (предпочтительно «Аккорд»), средства разграничения доступа («Аккорд-Win32» или «Аккорд-Win64»), средства управления доступом, серверы доверенного сеанса связи, при использовании средств виртуализации – СЗИ НСД «Аккорд-В.». Конечно, необходимы полномасштабные документы по политике информационной безопасности и построенная в соответствии с ними служба ИБ.

Для клиентов выбор шире. Рекомендации я бы разделил по масштабам бизнеса с обязательным созданием и контролем доверенной среды. Итак.

1. Для крупных предприятий на компьютерах, с помощью которых выполняется взаимодействие с банком, должны быть установлены и правильно настроены программно-аппаратные комплексы «Аккорд». Это меры необходимые, но их целесообразно дополнить «санитарной зоной» и периферийной защитой, соответствующими по производительности эксплуатируемой информационной системе.

2. Для средних предприятий, в которых компьютер используется не только для связи с банком, нужно устанавливать программно-аппаратный комплекс «Аккорд», дополненный переключателем SATA-интерфейсов. В этом случае можно обеспечить доверенную среду на время сеанса связи с банком, не теряя привычных особенностей среды функционирования.

3. Для небольших хозяйствующих субъектов, индивидуальных предпринимателей, физических лиц рекомендуем использовать средство обеспечения доверенного сеанса связи (СОДС) «МАРШ!». СОДС «МАРШ!» обеспечивает доверенный сеанс связи клиента с банком при минимальной стоимости и приемлемых функциональных характеристиках.

Один из вариантов СОДС «МАРШ!» специально предназначен для использования в ДБО. Это новое изделие, и мы здесь опишем его немного подробнее.

Обычный, широко используемый вариант СОДС «МАРШ!» – это активное USB-устройство с собственным микропроцессором, который осуществляет правильное управление памятью. Память надежным способом разбита на несколько разделов, в которых контролируемым образом размещаются операционная система, браузер, функциональное ПО, модуль интеграции с библиотекой электронной подписи и сама эта библиотека. «МАРШ!» – загрузочное устройство, целостность его содержимого обеспечивается технологически, и если загрузиться с него, то создается и поддерживается доверенная среда, достаточная для целей безопасного применения электронной подписи.

СОДС «МАРШ!» уже сейчас широко используется в корпоративных системах и показывает эффективность подхода.

По крайней мере, в ряде случаев решение на основе этого устройства в разы дешевле решений на основе сертифицированных электронных замков.

Если же планируется использовать «МАРШ!» в системах ДБО, где пользователь – физическое лицо, то он должен обладать хотя бы минимальными навыками по настройке сетевых подключений. Как оказалось, целый ряд пользователей этими навыками не владеет даже в минимальной степени.

Чтобы обеспечить комфортную работу этой категории пользователей, мы совместили решение «МАРШ!» и 3G модем в едином конструктиве. Получилось новое комплексное устройство, пользоваться которым не сложнее, чем телефоном, недорогое и, главное, привычное для пользователей. Миллионы людей уже используют беспроводные модемы и, таким образом, практически готовы к применению СОДС «МАРШ!». Получилось устройство в модном сегодня формате – все в одном. Если просто подключить его к компьютеру – получаем модем для беспроводного доступа к сети Интернет, если загрузиться с него – получаем безопасный доступ к управлению счетом.

Нам кажется, что в техническом смысле проблема решена. Остальное – только желание банков.

***НБЖ: Готовы ли клиенты банков пользоваться дополнительными системами безопасности, которые, возможно, сделают процесс обслуживания в системах ДБО менее удобным?***

**В. КОНЯВСКИЙ:** Клиенты готовы пользоваться теми средствами, которые обеспечивают безопасность бизнеса. Разговоры вроде «как же, станет еще бухгалтер делать то-то и то-то...» – это досужие разговоры вне сферы бизнеса. Не бухгалтер зарабатывает деньги для компании, и не бухгалтеру решать, что безопасно, а что нет. Не хочет выполнять требования по безопасности – пусть ищет другую работу. Требуемый уровень безопасности определяет собственник. Допускаю, что есть собственники, для которых комфорт бухгалтера важнее денег. Но этот случай не стоит серьезно рассматривать в качестве типового.

А вот помочь собственнику сделать правильный выбор достаточного уровня защищенности – это главная на сегодняшний день задача сообщества.

***НБЖ: Какие программные средства защиты на стороне клиента существуют на рынке?***

**В. КОНЯВСКИЙ:** Программные средства защиты не могут обеспечить никакого приемлемого уровня безопасности, это должны понять все. Не тратьте деньги зря, как бы вам ни хвалили любой программный продукт. Невозможно обеспечить защищенность без создания доверенной среды, и невозможно обеспечить создание доверенной среды без аппаратных средств. Эта аппаратура необязательно сложная и дорогая, но совсем без аппаратуры нельзя. И еще – годится не любая аппаратура, имеющая тот или иной сертификат. Нужны средства, которые обеспечивают создание доверенной среды. NBJ