

# Информационная безопасность финансового института

## Что предлагает рынок для защиты информации



Текст: Юрий Акаткин, временно исполняющий обязанности директора ФГУП «КБПМ»

Развитие банковских информационных технологий сопровождается постоянным совершенствованием технологий обеспечения информационной безопасности, которые обеспечивают конфиденциальность банковской информации, доступность и целостность информационных ресурсов, позволяют предотвратить возможный ущерб как для самих банков, так и для их клиентов. Последнее особенно важно для систем ДБО.

Поскольку в ДБО предусматривается взаимодействие с гражданами и круг участников взаимодействия не определен, такая базовая характеристика процесса информационного взаимодействия, как доверие, имеет особое значение. Доверять можно только известному участнику, а значит, перед началом процесса он должен идентифицироваться.

Клиент банка в ДБО взаимодействует с удаленным информационным ресурсом только для решения строго определенной задачи. И вместо того чтобы предпринимать дорогостоящие меры по созданию постоянной доверенной среды, достаточно было бы обеспечить доверенную среду выполнения этой задачи. То есть организовать доверенный сеанс связи (ДСС) для работы с ДБО. Суть концепции ДСС состоит в том, что необходимый уровень защищенности компьютера обеспечивается не на все время эксплуатации компьютерной системы, а только на то время, когда высокая защищенность

действительно необходима. Примером практической реализации этой концепции является средство обеспечения доверенного сеанса связи СОДС «МАРШ!» производства ОАО «ОКБ САПР» и ФГУП «КБПМ» (ГК «Ростехнологии»). При применении СОДС «МАРШ!» пользователю предоставляется уровень защиты близкий к уровню доверенного компьютера с набором сертифицированных ОС, СЗИ НСД и СКЗИ. СОДС «МАРШ!» состоит из клиентской и серверной частей – Клиента ДСС и Сервера ДСС. Клиент ДСС – загрузочное персональное устройство «МАРШ!», содержащее загрузочную ОС, набор функционального ПО, СЗИ НСД и СКЗИ. Сервер ДСС – доверенный сервер, обеспечивающий создание и работу защищенного сетевого соединения с пользователями, имеющими персональные устройства (Клиенты ДСС).

Конструктивно Клиент ДСС выполнен в виде USB-устройства, что позволяет использовать его практически со всеми компьютерами. «МАРШ!» представляет собой активное микропроцессорное устройство с многоконтурной криптографической подсистемой, проверенной защищенной операционной системой Linux, браузером, специальной подсистемой управления к памяти и многим другим. Память, в которой размещается все необходимое для работы программное обеспечение, технологически разбита на разделы с разными атрибутами доступа. Это позволяет исключить несанкционированные модификации критичного ПО и одновременно обеспечить все необходимые режимы с памятью.

«МАРШ!» как средство обеспечения доверенного сеанса связи включает в себя следующие возможности:

- полноценную криптозащиту;
- возможность работы на любом компьютере в обычном режиме и в режиме ДСС;
- приемлемую стоимость и минимальные затраты в процессе эксплуатации;
- простоту использования, мобильность и компактность;
- выбор оптимальной конфигурации в соответствии с требованиями заказчика.

Важно отметить, что СОДС «МАРШ!» может эффективно использоваться как средство электронной подписи, то есть в варианте СЭП. Начиная доверенный сеанс связи, пользователь (клиент банка) загружается на произвольном компьютере с СОДС «МАРШ!», обеспечивая тем самым доверенную вычислительную среду. В этой среде стартует браузер и все сопутствующее программное обеспечение, необходимое для работы, устанавливается защищенное соединение с сервером ДСС удаленной защищенной информационной системы ДБО (закрытые ключи и сертификаты хранятся в защищенной памяти «МАРШ!»). В рамках доверенного сеанса связи обеспечивается защищенный обмен информацией между банком и клиентом с соблюдением всех требований № 63-ФЗ «Об электронной подписи».

Во время доверенного сеанса связи с банком пользователю гарантирована недоступность ресурсов компьютера, а также внешние соединения (сеть Интернет), которые могут быть потенциально небезопасными. Однако, закончив работу с защищенной информационной системой и перезагрузив компьютер, пользователь может продолжить работу в обычном режиме. При этом никакие из используемых им ресурсов не смогут оказать влияния на взаимодействие с банком.

В настоящее время использование СЭП «МАРШ!» отработано совместно с ЗАО «РФК» (Российские финансовые коммуникации) для варианта применения с системами ДБО «Спектр» и «Клиент-WEB».

Стоимость СЭП «МАРШ!» в разы ниже стоимости существующих традиционных решений, накладывающих к тому же массу ограничений на привычную работу с защищенным компьютером.

Проведенные испытания показали, что «МАРШ!» может быть адаптирован к различным системам ДБО, существенно повышая их безопасность и эффективность при минимальных затратах. Сегодня СЭП «МАРШ!» не имеет аналогов на рынке. Это уникальное решение имеет все шансы стать эталоном защиты в системах ДБО. <sup>№3</sup>