Круглый стол «Как уберечь средства клиентов, если обслуживание предприятий осуществляется банком дистанционно»

С развитием дистанционного банковского обслуживания растет и уровень угроз для пользователей систем ДБО: у банков деньги похитить можно, и мошенники с успехом воруют деньги и в новых условиях. О том, как этого не допустить, мы беседуем с экспертами и участниками рынка.

Веселов Александр,
ведущий инженер ЗАО «С-Терра СиЭсПи»

Вопрос 1. *Какие средства и системы обеспечения безопасности систем ДБО могут применяться на стороне исключительно банка, во взаимной работе банка и клиента, и исключительно на стороне клиента?*

Александр Веселов: Интернет-технологии настолько прочно вошли в нашу жизнь, что мы пользуемся он-лайн услугами везде и всегда. Системы ДБО также предоставляют клиентам возможность подключения как со стационарного компьютера или ноутбука, так и с мобильного телефона или планшета. Такое многообразие способов доступа порождает множество угроз, как для пользователя, так и для банка.

В этих условиях нецелесообразно защищать один компонент системы и оставить беззащитным другой, так как обязательно найдется злоумышленник, который этим воспользуется. Поэтому средства обеспечения безопасности необходимо применять и на стороне банка, и на стороне клиента.

На стороне банка обычно используется так называемая «периметровая» защита с несколькими контурами. Контуры могут быть разделены по функциональному признаку (межсетевой экран, VPN-шлюз, контекстный фильтр), а также по производителям.

Более надежно для защиты периметра банка использовать продукцию российских компаний, например, «С-Терра СиЭсПи», выполненную в соответствии с требованиями регуляторов (ФСБ, ФСТЭК, Банка России). Ведь в последнее время регулярно появляется информация о компрометации продуктов некоторых западных производителей, в том числе речь идет и о средствах защиты информации.

Банковское оборудование располагается в контролируемой зоне, поэтому большинство угроз, связанных с несанкционированным физическим доступом, не являются актуальными. Наиболее часто в последнее время приходится сталкиваться с атаками типа «отказ в обслуживании», когда злоумышленники атакуют банковские серверы и парализуют работу легитимных пользователей. В остальном, подавляющее большинство атак направлено не на банк, а на пользователя. Ведь защита его рабочего места на порядок слабее системы защиты серверов банка.

Как правило, на стороне пользователя применение организационных средств защиты неэффективно – большинство пользователей игнорируют регламенты и инструкции. Поэтому необходимо простое и, в тоже время, надежное средство защиты, которое сможет использовать неквалифицированный пользователь.

Вопрос 2. *- Насколько, на ваш взгляд, сегодня эффективны «традиционные» системы обеспечения безопасности ДБО: аутентификация по логину-паролю, шифрование, электронная подпись?*

Александр Веселов: Информационная безопасность – это комплексное, многогранное понятие, которое предполагает системный подход к нейтрализации угроз. Мы уже говорили о том, что не имеет смысла защищать одну часть системы и не защищать другую, так как злоумышленник использует наименее защищенное звено.

Самым уязвимым компонентом системы ДБО является пользователь. Как правило, он обладает низкой квалификацией в сфере информационной безопасности, поэтому чаще всего подвергается атакам злоумышленников. В такой ситуации «традиционные» меры обеспечения безопасности являются необходимыми, но недостаточными. Они корректно выполняют поставленные перед ними задачи, но требуется дополнительная защита. Это может быть антивирусное ПО, внешние ключевые носители, средство доверенной загрузки и другие. Однако, ситуация усугубляется сложностью эксплуатации средств защиты. Пользователь может отключить их, некорректно изменить настройки и т.д. В такой ситуации требуется надежное средство обеспечения безопасности с максимально простым сценарием использования и, в то же время, с высоким уровнем защиты. Одним из таких решений является устройство, основанное на технологии среды построения доверенного сеанса, – СПДС «ПОСТ» производства компании «С-Терра СиЭсПи».

Вопрос 3. *Насколько эффективны решения, предполагающие организацию «доверенной среды» для работы системы ДБО, например, загрузка специально сформированной операционной системы с доверенного носителя с дальнейшим поднятием VPN-соединения с сервером банка и запуском системы ДБО? Как в этом случае можно организовать безопасное взаимодействие с системой ДБО «бухгалтерских» систем?*

Александр Веселов: В условиях, когда пользователь на одном и том же рабочем месте обращается к ресурсам банка и просматривает Интернет-страницы, обеспечить полноценную защиту не представляется возможным. Ранее в такой ситуации использовали отдельную рабочую станцию (например, «компьютер бухгалтера»), а сейчас появилось более универсальное решение – технология среды построения «доверенного сеанса». Одним из продуктов этого сегмента является устройство СПДС «ПОСТ» производства компании «С-Терра СиЭсПи» - компактное (размером с обычную USB-флешку) средство, обеспечивающее высочайший уровень безопасности при работе в системе ДБО.

Пользователь (клиент ДБО) загружает эталонную операционную систему с защищенного USB-носителя, при загрузке вводит пин-код. Далее устанавливается защищенное соединение с информационной системой банка. Передаваемая информация шифруется с помощью отечественных криптоалгоритмов ГОСТ. Пользователь работает с ресурсами банка в изолированной среде, взаимодействие осуществляется через VPN-туннель. При этом исключено нарушение конфиденциальности и целостности информации при её передаче. При таком подходе у пользователя минимум привилегий – он не может отключить средство защиты или запустить стороннее ПО.

СПДС «ПОСТ» позволяет обеспечить аппаратную защиту с помощью смарт-карты, полную изоляцию от потенциально опасных ресурсов рабочей станции, запрет доступа в интернет и т.д.

Злоумышленник не сможет получить доступ к данным пользователя и ресурсам банка даже при потере или краже устройства – без знания пин-кода «прочитать» данные невозможно, а количество

попыток ввода ограничено. Кроме того, при потере устройства администратор «закрывает» доступ с этого носителя к ресурсам банка с помощью отзыва сертификата.

Немаловажным является наличие у продукта СПДС «ПОСТ» сертификата ФСБ РФ по классу КС2, что полностью соответствует требованиям СТО БР ИББС.

Такой подход позволяет защитить не только взаимодействие между клиентом и банком, но и организовать полноценную защиту рабочего места пользователя. При этом система будет соответствовать требованиям отраслевого регулятора – Банка России.

Вопрос 4. *Насколько эффективна двухфакторная аутентификация либо двухфакторное подтверждение операций (с помощью ввода sms-пароля, кода скрэтч-карты, usb-токена и т.д.)?*

Александр Веселов: Практика показывает, что для нейтрализации актуальных угроз в системах ДБО явно недостаточно однофакторной аутентификации, она создает лишь иллюзию защиты. Поэтому двухфакторная аутентификация – обязательный атрибут современной системы безопасности. Наиболее популярная реализация – sms-подтверждение входа в систему клиент-банк или проведения операции со счетом.

При использовании технологии СПДС (среда построения доверенного сеанса) двухфакторная аутентификация является неотъемлемой частью сценария доступа пользователя к целевым ресурсам. Первый фактор – наличие защищенного USB-носителя, второй – знание пин-кода для загрузки операционной системы.

При этом подтверждение операций посредством sms может стать дополнительным инструментом защиты.

Вопрос 5. *- Какие новшества Вы внедрили в области защиты систем ДБО за последний год?*

Александр Веселов: Компания «С-Терра СиЭсПи» является одним из лидеров по производству средств защиты информации для банковского сектора. Достигается это за счет использования международных стандартов IKE/IPsec и соответствия отечественному законодательству. Наши VPN-шлюзы уже давно используются во многих банках, администраторы привыкли к интерфейсу, аналогичному Cisco IOS. Поэтому пилотные проекты с новым средством для защищенного удаленного доступа, СПДС «ПОСТ», проходят достаточно легко, несмотря на особенности системы защиты каждого банка. На основе этих пилотных проектов нам удалось значительно доработать продукт, учитывая банковскую специфику. СПДС «ПОСТ» только завоевывает рынок, но уже сейчас можно говорить о том, что среда построения доверенного сеанса – это более современный и надежный подход к защите ДБО, чем «традиционные» меры защиты.