Меры информационной безопасности

Технологии и средства обеспечения информационной безопасности проводимых операций в системе дистанционного банковского обслуживания ООО «ЖИВАГО БАНК»:

- шифрование трафика, передающегося между клиентом и сервером, с помощью протокола SSL (Secure Sockets Layer). Этот режим защиты позволяет обеспечить конфиденциальность передаваемых данных при работе в системе ДБО;
- механизм авторизации (предоставление доступа) в системе ДБО обеспечивает идентификацию и аутентификацию пользователей по системному имени (логину) и паролю;
- для защиты от фальсификации передаваемого по каналам связи электронного документа в системе ДБО используются средства электронной подписи (ЭП), позволяющие идентифицировать владельца ключа проверки электронной подписи, а также установить отсутствие искажения информации в документе. Используемые в системе ДБО ООО «ЖИВАГО БАНК» средства ЭП сертифицированы ФСБ РФ;
- все события в системе ДБО протоколируются. Администраторы системы имеют возможность просмотра протокола событий в системе.

Перечень нормативно-правовых актов, регламентирующих использование этих технологий и средств:

1. «Доктрина информационной безопасности Российской Федерации», утв. Президентом РФ 09.09.2000 г. № Пр-1895;
2. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 г.;
3. Указ Президента РФ «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» № 334 от 03.04.1995 г.;
4. Федеральный закон РФ «Об электронной подписи» № 63-ФЗ от 06.04.2011 г.;
5. Постановление Правительства РФ «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» № 313 от 16.04.2012 г.;
6. «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ–2005)», утв. приказом ФСБ РФ № 66 от 09.02.2005 г.;
7. «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утв. приказом ФАПСИ при Президенте РФ № 152 от 13.06.2001 г.

Меры информационной безопасности, которые рекомендуется применять клиентам ООО «ЖИВАГО БАНК», пользующимся услугами дистанционного банковского обслуживания:

- электронная подпись руководителя организации под электронным расчетным платежным документом вырабатывается с использованием ключевого носителя. Право доступа к ключевому носителю фактически означает право ставить подпись от имени руководителя организации. Учет и хранение ключей электронной подписи должно быть поручено специально уполномоченным сотрудникам;
- место хранения ключевых носителей с ключами ЭП (сейф, металлический шкаф и т.д.) должно обеспечивать их безопасность и надежную защиту от несанкционированного доступа посторонних лиц;
- извлекайте из компьютера съемный носитель, содержащий ключи ЭП, сразу после завершения работы в Системе ДБО;
- не записывайте на носитель, содержащий ключи ЭП, какую-либо другую информацию. Не пишите на ключевом носителе свой логин и пароль для входа в систему «Интернет–Банк»;
- категорически запрещается хранить ключи ЭП на жестком диске компьютера;
- исключите неконтролируемое копирование ключевого носителя;
- проводите полную антивирусную проверку ПЭВМ, с которой ведется работа в Системе ДБО. Возможно, на вашем компьютере находятся вредоносные программы, которые дают возможность злоумышленникам управлять вашим компьютером посредством удаленного доступа к нему. Если на вашем компьютере не установлены лицензионные средства антивирусной защиты, настоятельно рекомендуем приобрести данные средства (антивирус Kaspersky, Eset NOD32, Dr. Web и др.), установить и настроить их на рабочем месте таким образом, чтобы осуществлялось ежедневное автоматическое обновление антивирусных баз и ежедневная антивирусная проверка;
- никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, полученные по электронной почте. Подозрительные файлы лучше немедленно удалять. Проверяйте все новые файлы, сохраняемые на компьютере;
- внимательно следите за программной и аппаратной конфигурацией Вашего компьютера. Если на компьютере появились новые программы, об установке которых Вы не имеете информации, то не следует работать в Системе ДБО до полного удаления этих программ. Если на компьютере появились новые устройства (жесткие диски, съемные накопители, сетевые карты), о подключении которых Вы не имеете информации, то не следует работать в Системе ДБО до отключения этих устройств;
- используйте только лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечивайте автоматическое обновление системного и прикладного программного обеспечения с сайтов производителей данного программного обеспечения, а также исключайте установку развлекательных и игровых программ;
- не предоставляйте общий доступ к жесткому диску компьютера, на котором установлена Система ДБО, исключите использование средств удаленного администрирования компьютера, в том числе встроенных в операционную систему (например, удаленное управление рабочим столом);
- не открывайте подозрительные файлы, присланные вам по электронной почте. В случае получения по электронной почте якобы от банка любых сообщений, содержащих вложенные файлы или ссылки на какие-либо Интернет-ресурсы, не открывайте вложения и не переходите по ссылке. Следует позвонить в банк по телефону не из

поступившего сообщения, а известному из других проверенных источников, и получить разъяснения о достоверности содержащейся в нем информации;

- запретите в электронной почте прием сообщений, содержащих исполняемые вложения;
- периодически, согласно настройкам Системы ДБО, меняйте пароль для входа в систему «Интернет–Банк». Пароль следует запомнить. Его хранение в письменном виде не рекомендуется, так как при этом возникает возможность доступа к паролю неуполномоченных лиц. Пароль должен быть не менее 8 символов, он не должен быть слишком простым, не рекомендуется использовать имена, числа и даты, связанные с владельцем пароля;
- обязательно пользуйтесь виртуальной клавиатурой, защищающей ваши логины и пароли от хищения при вводе;
- на компьютерах, используемых для работы в Системе ДБО, исключите посещение всех Интернет-сайтов непроизводственного характера (конференции, чаты, социальные сети, телефонные сервисы, новостные сайты, сайты сомнительного содержания), кроме используемых для входа в Систему ДБО и доверенных ресурсов сети Интернет, необходимых для выполнения должностных обязанностей. Перед началом работы в Системе ДБО закрывайте все открытые интернет-страницы. По окончанию работы с системой также следует закрыть окно интернет-браузера;
- контролируйте имя Интернет-сервера Банка при входе в Систему ДБО. Имя Интернет-сервера банка https://dbo.zhivagobank.ru. Помните, что сайты, визуально напоминающие сайт Системы ДБО, создаются специально для незаконного получения информации. В случае обнаружения фальсифицированного сайта, копирующего дизайн официального сайта ООО «ЖИВАГО БАНК» или Системы ДБО, пожалуйста, незамедлительно сообщите об этом по контактным телефонам Банка. Список адресов (доменных имен) официальных WEB-сайтов банка размещен на сайте Банка России по адресу http://www.cbr.ru/credit/CO_SitesFull.asp. Если Вы обнаружили в сети Интернет ложные web-сайты ООО «ЖИВАГО БАНК» или с Вами пытаются связаться по электронной почте или иным способом с требованиями о предоставлении персональных идентификаторов доступа к Системе ДБО, просьба немедленно сообщить об этом в банк;
- в случае возникновения трудностей при включении компьютера, загрузке операционной системы, при подключении к Системе ДБО, Интернету, или нестабильном функционировании компьютера, на котором установлена Система ДБО (более медленная, чем обычно работа, произвольная перезагрузка, другие неполадки) немедленно сообщайте об этом в банк;
- риск хищения и дальнейшего неправомерного использования ключа ЭП и другой аутентификационной информации при доступе к Системе ДБО увеличивается в случае работы на гостевых рабочих местах (интернет-кафе и т.д.).