Краткое описание технологий и средств обеспечения информационной безопасности применяемых систем ДБО

Система «Банк-Клиент» предлагает своим пользователям не только широкий спектр дистанционных банковских услуг, но и гарантирует конфиденциальность и безопасность передачи данных при работе в сервисе.

Безопасность обеспечивается следующими компонентами защиты:

- криптографический протокол шифрования информации при обмене данными между клиентом и Интернет-банком (передача конфиденциальной информации между клиентом и Банком посредством сетей общего доступа происходит по шифрованному каналу передачи данных. Для защиты от несанкционированного доступа в телекоммуникационных каналах используются протокол Transport Layer Security (TLS) с длиной сессионного ключа не менее 128 бит, а соединение браузера клиента и сервера ДБО осуществляется по протоколу HTTPS);
- двухфакторная аутентификация клиента Интернет-банка (Авторизация клиента в Интернет-банке производиться на основании его логина и пароля. Для входа в Интернет-банк и подтверждения клиентом правильности, неизменности и целостности отправляемых распоряжений на выполнение операций в Интернет- банке используется одноразовый секретный пароль, высылаемый клиенту на его номер мобильного телефона в виде SMS- или PUSH-сообщения);
- возможность использования виртуальной клавиатуры для ввода пароля (Данная технология повышает степень защищенности пароля от вирусов-кейлоггеров (клавиатурных перехватчиков), которые запоминают и пересылают данные, введенные с клавиатуры компьютера.);
- организационно-административные мероприятия;
- криптографические средства защиты информации;
- ограничение по времени бездействия в системе во избежание использования Интернет-банка третьими лицами;
- использование альтернативного канала связи для подтверждения каждой операции в Интернет-банке (подтверждение действительным разовым паролем (высылается клиенту на мобильный номер в виде SMS- или PUSH-сообщения) любых операций в Интернет-банке);
- применение средств защиты ОС и СУБД, в том числе штатных;
- системы контроля доступа;
- системы межсетевого экранирования, фильтрация и маршрутизация трафика систем ДБО.

Перечень законодательных и иных актов, регламентирующих использование технологий и средств обеспечения информационной безопасности применяемых систем ДБО

1. Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
2. Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»;
3. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»;
4. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
5. Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности";
6. Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи";
7. Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании";
8. Федеральный закон от 07.07.2003 N 126-ФЗ "О связи";
9. Указ Президента РФ от 03.04.1995 N 334 "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации";
10. Указ Президента РФ от 17.03.2008 N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";
11. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Перечень сведений конфиденциального характера»;
12. Постановление Правительства РФ от 16.04.2012 N 313 "Об утверждении Положения о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами";
13. Постановление Правительства РФ от 21.11.2011 N 957 "Об организации лицензирования отдельных видов деятельности";

14. Постановление Правительства РФ №687 от 15.09.2008г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
15. Постановление Правительства РФ №512 от 06.07.2008г. «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
16. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
17. Постановление Банка России от 9 июня 2012 г. № 382-П «О требованиях по обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»;
18. Постановление Банка России от 9 июня 2012 г. № 381-П "Положение о порядке осуществления надзора за соблюдением не являющимися кредитными организациями операторами платежных систем, операторами услуг платежной инфраструктуры требований Федерального закона от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе", принятых в соответствии с ним нормативных актов Банка России";
19. "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.";
20. "Временное Положение о порядке приема к исполнению поручений владельцев счетов, подписанных аналогами собственноручной подписи, при проведении безналичных расчетов кредитными организациями" (утв. Банком России 10.02.1998 N 17-П);
21. "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.;
22. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности» РС БР ИББС- 2.5-2014"
23. Приказ ФСБ, ФСТЭК №416/489 от 31.08.2010г. «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»;
24. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г., № 149/6/6-622;
25. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г., № 149/54-144;
26. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;
27. ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма»;
28. ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
29. Письмо Банка России от 27.04.2007 N 60-Т "Об особенностях обслуживания кредитными организациями клиентов с использованием технологии дистанционного доступа к банковскому счету клиента (включая интернет- банкинг)";
30. Письмо Банка России от 07.12.2007 N 197-Т "О рисках при дистанционном банковском обслуживании";
31. Письмо Банка России от 31.03.2008 N 36-Т "О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем Интернет-банкинга";
32. Письмо Банка России от 30.01.2009 N 11-Т "О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга";
33. Письмо Банка России от 30.08.2006 N 115-Т "Об исполнении Федерального закона "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" в части идентификации клиентов, обслуживаемых с

использованием технологий дистанционного банковского обслуживания (включая интернет-банкинг)";
34. Письмо Банка России от 05.04.2007 N 44-Т "О проверке осуществления кредитными организациями идентификации клиентов, обслуживаемых с использованием технологий дистанционного банковского обслуживания (включая интернет-банкинг)";
35. Указание Банка России № 3007-У «О внесении изменений в Положение Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»;
36. Письмо Банка России от 05.08.2013 N 146-Т «О рекомендациях по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети «Интернет»;
37. Другие федеральные законы и принимаемые в соответствии с ними иные нормативные правовые акты Российской Федерации, а также существующие соглашения сторон.