Краткое описание технологий и средств обеспечения информационной безопасности применяемых систем ДБО

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

- Конституция РФ от 12 декабря 1993 г.;

2. Кодексы:

- Гражданский кодекс РФГК РФ) от 30.11.1994 № 51-ФЗ;

3. Доктрины:

- «Доктрина информационной безопасности РФ» (утв. Президентом РФ 09.09.2000 N Пр-1895);

4. Федеральные законы:

- Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»;
- Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»;
- Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Федеральный закон от 04.05.2011 N 99-ФЗ «О лицензировании отдельных видов деятельности»;
- Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 27.12.2002 N 184-ФЗ «О техническом регулировании»;
- Федеральный закон от 07.07.2003 N 126-ФЗ «О связи».

5. Указы:

- 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»;
- 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»;
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Перечень сведений конфиденциального характера».

6. Постановления:

- Постановление Правительства РФ от 16.04.2012 N 313 «Об утверждении Положения о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;
- Постановление Правительства РФ от 21.11.2011 N 957 «Об организации лицензирования отдельных видов деятельности»;
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ №687 от 15.09.2008г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- 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»;
- 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»;
- 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»

7. Положения, инструкции, стандарты, приказы, руководящие документы, требования, методические рекомендации:

- «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.»
- «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);
- «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.;

- Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014″ СТО БР ИББС-1.2-2014″ (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399
- Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014″ (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399);
- Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 N 28375);
- Руководящий документ ФСТЭК России от 15.02.2008г. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Руководящий документ ФСТЭК от 14.02.2008г. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ, ФСТЭК №416/489 от 31.08.2010г. «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»;
- 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;
- Требования к средствам криптографической защиты конфиденциальной информации, ФСБ России, Москва;
- 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;
- ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;
- ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма»;
- ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
- Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности» РС БР ИББС-2.5-2014 (приняты и введены в действие Распоряжением Банка России от 17.05.2014 N Р-400);
- Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» РС БР ИББС-2.2-2009 (приняты и введены в действие Распоряжением Банка России от 11.11.2009 N Р-1190);
- Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0″ РС БР ИББС-2.0-2007 (приняты и введены в действие Распоряжением Банка России от 28.04.2007 N Р-348);
- Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0″ РС БР ИББС-2.1-2007 (приняты и введены в действие Распоряжением Банка России от 28.04.2007 N Р-347);
- Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации» (утв. Банком России, АРБ, Ассоциацией региональных банков России (Ассоциация «Россия»);

8. Письма, указания ЦБ РФ:

- 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)»;
- Письмо Банка России от 07.12.2007 N 197-Т «О рисках при дистанционном банковском обслуживании»;
- 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»;
- 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»;
- 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)»;
- 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)»;
- 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»

9. Другие федеральные законы и принимаемые в соответствии с ними иные нормативные правовые акты Российской Федерации, а также осуществляется соглашение сторон.

Краткое описание технологий и средств обеспечения информационной безопасности применяемых систем ДБО (Интернет сервис)

ДБО (Дистанционное банковское обслуживание) — удобный и современный способ управления финансовыми потоками по различным каналам связи (телефонные или выделенные линии, сеть Интернет).Преимущества Систем ДБО:

- Простое и удобное в обращении программное обеспечение, не требующее от пользователя особых знаний и навыков.
- Минимизация ошибок при заполнении платежных документов.
- Возможность обработки и передачи большого количества документов; высокий уровень защиты данных, возможность шифрования/дешифрования информации.

Система **«Интернет-Клиент-Банк»** — система дистанционного банковского обслуживания (ДБО) АРКБ «РосБизнесБанк» (ПАО) представляющие собой многофункциональные программно-технологические комплексы, которые отличает (сочетают в себе):

- Удобство интерфейса;
- Простоту работы;
- Предоставление полной расширенной информации по счету за весь срок работы клиента с даты открытия расчетного счета;
- Работу в браузере Internet Explorer и Google Crome;
- Позволяет делать импорт и экспорт документов из системы ДБО в системы бухгалтерского учета 1С предприятия или в любую другую систему посредством импорта в собственный стандарт выгрузки (в этом случае клиентом нужна доработка своего программного обеспечения);
- Система позволяют использовать в работе любое количество ЭП клиента проставляемые на документы. Это дает гибкость контроля прохождения документов от предприятия в банк с последующим возможным контролем руководителя предприятия всех платежей уходящих по системе дистанционного банковского обслуживания.

Меры обеспечения безопасности системы ДБО

АРКБ «РосБизнесБанк» (ПАО) применяет самые современные технологии, позволяющие обеспечить максимальную безопасность при использовании электронного документооборота, как юридических лиц и индивидуальных предпринимателей, так и физических лиц. Программное обеспечение отвечает всем требованиям Российского законодательства в области защиты информации.Для обеспечения информационной безопасности системы ДБО банк использует только сертифицированные средства защиты информации российских разработчиков.Безопасность и защита от несанкционированного доступа в системе ДБО обеспечивается применением в комплексе:

- Криптографических средств защиты информации (Максимальная степень защиты сертифицированными ФСБ средствами защиты информации на базе СКЗИ «КриптоПРО»);
- Аутентификации, авторизации, протоколирования (Аутентификация клиента происходит с несколькими этапами защиты посредством сертифицированного программно-аппаратного средства аутентификации и хранения ключевой информации электронного ключа USB носителя);
- Организационно-административных мероприятий;
- Средств защиты ОС и СУБД (антивирусных средств, средств обнаружения вторжений и т.д.);
- Периодического контроля;
- Электронной подписи (Электронная подпись (ЭП) документов основана на ГОСТ 34.10-2001, что полностью соответствует требованием Федеральной службы безопасности Российской Федерации в области криптографической защиты информации);
- Межсетевого экранирования (Межсетевые экраны призваны контролировать доступ клиентов из сети Интернет к ресурсам, находящимся в сети банка);
- Систем контроля доступа;
- Фильтрации трафика, относящегося к системам ДБО и его маршрутизация;
- Шифрования трафика (Передача конфиденциальной информации между клиентом и банком посредством сетей общедоступного доступа INTERNET происходит по шифрованному каналу передачи данных. При шифрации используется сертифицированные российские алгоритмы шифрования по ГОСТ 28147-89). Для защиты от несанкционированного доступа в телекоммуникационных каналах используются протоколы Transport Layer Security (TLS) и Secure Socket Layer (SSL 3.0) с длиной сессионного ключа не менее 128 бит, а соединение браузера клиента и сервера **«Интернет-Клиент-банк»** осуществляется протоколом HTTPS);
- Периодической аттестации объектов информатизации (ДБО).

Лицензии банка на осуществление видов деятельности (на предоставление услуг ДБО)

На осуществление разработки, производства, распространения 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) ЛСЗ №0006562 рег.№1341Н от 14 июня 2014 г.

Меры информационной безопасности, которые рекомендуется применять клиентам ПАО АРКБ «РосБизнесБанк», пользующимся услугами дистанционного банковского обслуживания

Уважаемый Клиент, АРКБ «РосБизнесБанк» (ПАО) постоянно совершенствует комплексную защиту системы дистанционного банковского обслуживания (далее – Система ДБО), поскольку любые операции с использованием Интернета сопряжены с рисками, в том числе угрозами хакерских атак и несанкционированного доступа к денежным средствам. Проводимые нами мероприятия по обеспечению высокого уровня безопасности Вашей финансовой информации опираются на новейшие технологии и методики. Система ДБО – качественный, современный и безопасный инструмент удаленного доступа к Вашим счетам и продуктам Банка при условии выполнения Вами следующих рекомендаций:

- Установите, настройте и регулярно обновляйте лицензионное антивирусное программное обеспечение на Вашем компьютере. Действие вирусов может быть направлено на перехват Вашей персональной информации и передаче её злоумышленникам.
- Осуществляйте периодическую проверку ПЭВМ средствами антивирусной защиты на предмет нахождения вирусов и других вредоносных программ;
- Используйте только лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.) Своевременно устанавливайте обновления операционной системы своего компьютера, рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей. Регулярно выполняйте обновления (патчи) операционной системы и браузера Вашего компьютера, так как данные действия значительно повысит его уровень безопасности. Также исключайте установку развлекательных и игровых программ;
- Установите и настройте персональный брандмауэр (firewall) на Вашем компьютере. Это позволит Вам запретить несанкционированный удаленный доступ к Вашему компьютеру из сети Интернет и Вашей локальной сети с использованием удаленного управления компьютером и терминального доступа. Дополнительно можно настроить брандмауэр на доступ только по адресам Системы ДБО .
- Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты Вашего компьютера – программы поиска шпионских компонент, программы защиты от «спам» — рассылок.
- 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 секретных ключей должно быть поручено специально уполномоченным сотрудникам;
- Храните ключи только на сертифицированном съемном USB носителе. Хранение ключевых носителей должно быть организовано в месте, недоступном для посторонних лиц и должно обеспечивать их безопасность и надежную защиту от несанкционированного доступа (сейф, металлический запирающийся шкаф и т.д.). Установка ключевых носителей на рабочее место допускается только непосредственно на время работы с Системой ДБО.
  ВАЖНО: После окончания сеанса работы в Системе ДБО съемный ключевой носитель должен быть незамедлительно извлечен из компьютера!
- Категорически запрещается хранить секретные ключи ЭП на жестком диске компьютера;
- Исключите неконтролируемое копирование ключевого носителя;
- Копирование ключевых носителей возможно только в целях резервирования, при этом резервные носители должны храниться в недоступном для посторонних лиц месте и использоваться только в случае порчи основного носителя;
- Если Вы используете несколько ключей при работе в системе ДБО (например первая и вторая подписи) — не переносите эти ключи на один ключевой носитель, а также не подключайте одновременно различные ключевые носители к компьютеру.
- Для контроля доступа к съемному ключевому носителю рекомендуется на него установить пароль.
  ВАЖНО: Не сообщайте никому пароль для доступа к съемному ключевому носителю (включая сотрудников Банка и сотрудников Вашей организации или Ваших родственников)!
- После окончания работы в Системе ДБО обязательно корректно завершите работу (выйдите из Системы ДБО с использованием кнопки «Выход») и/или закройте WEB браузер.
- **ВАЖНО**: Извлеките из компьютера съемный ключевой носитель!
- Производите замену ключей ЭП до истечения срока их действия. Кроме того, проводите замену ключей ЭП во всех случаях увольнения и/или смены лиц, имеющих доступ к Системе ДБО, а также в случаях увольнения и/или смены лиц — руководителей с правом подписи доверенностей на получение ключей ЭП, и в случае подозрений на их компрометацию.
- В обязательном порядке следует отключать Автозапуск в операционной системе (для OS Windows: «Панель управления» -> «Администрирование» -> «Службы»; необходимо найти в закладке «Расширенный» службу «Определение оборудования оболочки» и установить «Отключено»);
- Исключите посещение с Вашего компьютера сайтов сомнительного содержания и любых других Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы и т.д.), а также чтение почты и открытие почтовых документов от недостоверных источников.
- На компьютерах, используемых для работы в Системе ДБО, исключите посещение всех Интернет-сайтов, кроме используемых для входа в Систему. Перед началом работы в Системе ДБО закрывайте все открытые интернет-страницы. По окончанию работы с системой также следует закрыть окно интернет-браузера;

- Категорически не рекомендуется работать с Системой ДБО из мест, не заслуживающих доверия (интернет-кафе и т.п.) или с использованием общественных каналов связи (бесплатный Wi-Fi и т.п.), так как это существенно увеличивает риск кражи Ваших персональных данных.
- Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях.
- На компьютере не рекомендуется устанавливать иное программное обеспечение, кроме необходимого для работы в Системе ДБО. Рекомендуется использовать для работы с Банком выделенный компьютер.
- Права пользователя, работающего с Системой ДБО, на данном компьютере должны быть минимально необходимыми (наличие прав администратора нежелательно).
- Не привлекайте для администрирования и обслуживания компьютера с установленной на нем Системой ДБО технических специалистов на условиях предоставления им удаленного доступа к компьютеру.
- Логины и пароли для работы в Системе ДБО – это Ваша персональная конфиденциальная информация. Ни при каких обстоятельствах не раскрывайте свой логин и пароль никому, включая сотрудников Банка. При обращении от имени Банка по телефону, электронной почте, через SMS лиц с просьбами сообщить конфиденциальную информацию (пароли, кодовые слова, и т.д.) ни при каких обстоятельствах не следует сообщать данную информацию.
- Периодически, согласно настройкам Системы ДБО, меняйте пароль для входа в Систему ДБО. Пароль следует запомнить. Пароль должен быть не менее 8 символов (4 цифровых и 4 буквеных символа), он не должен быть слишком простым, не рекомендуется использовать имена, числа и даты, связанные с владельцем пароля; менять пароль рекомендуется раз в месяц;
- Не сохраняйте Ваш логин и пароль в письменном виде, а также в текстовых файлах на жестком диске компьютера, либо на других электронных носителях информации, т.к. при этом существует риск его кражи и компрометации.
- Не записывайте на носитель, содержащий секретные ключи ЭП, какую-либо другую информацию. Не пишите на ключевом носителе свой логин и пароль для входа в Систему ДБО;
- Обязательно пользуйтесь виртуальной клавиатурой, защищающей ваши логины и пароли от хищения при вводе;
- В случае сбоев в работе компьютера или его поломки во время/после работы с Системой ДБО (проблемы с загрузкой операционной системы, выход из строя жесткого диска, и т.п.), следует **НЕМЕДЛЕННО** извлечь ключи и выключить компьютер, а также обратиться в Банк и убедиться, что от Вашего имени не производились несанкционированные операции.
- Обращайте внимание на любые изменения в привычных для Вас процессах установления соединения с Системой ДБО или в функционировании Системы ДБО. При возникновении любых сомнений в правильности функционирования Системы ДБО незамедлительно обратитесь в Банк.
- При работе с Системой ДБО (**«Интернет-Клиент-Банк»**) убедитесь, что защищенное соединение по протоколу https установлено именно с официальным сайтом услуги. Настоятельно не рекомендуется переходить на данную страницу по ссылке с Интернет-ресурсов (за исключением официального ресурса Банка, www.rbb.ru) или поступивших по электронной почте писем.
  ВНИМАНИЕ! Незамедлительное обращение в Банк с предоставлением полной информации о несанкционированном списании денежных средств со счетов может позволить оперативно приостановить операции и предотвратить финансовые потери.
  При любых подозрениях на мошеннические действия (компрометацию ключей электронной подписи, логинов, паролей и т.д.), а так же при нестабильной работе Системы ДБО (зависание Системы ДБО, самопроизвольное выключение Системы ДБО и т.д.), следует незамедлительно прекратить работу в Системе ДБО, извлечь из компьютера ключевой носитель, и обратиться в Банк по телефону Службы технической поддержки: **(495) 645-61-51 (239).**