ПРАВИЛА
информационной безопасности при работе в системе дистанционного банковского обслуживания

1. Общие положения

1.1. Термины и определения.

Злоумышленник - лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий.

Злоумышленные действия – любые действия, совершаемые Злоумышленником в Системе.

Угроза - опасность, предполагающая возможность потерь (ущерба).

Риск - мера, учитывающая вероятность реализации Угрозы и величину потерь (ущерба) от реализации этой Угрозы.

Информационная безопасность - безопасность, связанная с Угрозами в информационной сфере. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

Защитная мера - сложившаяся практика, процедура или механизм, которые используются для уменьшения Риска нарушения Информационной безопасности в Системе.

Инцидент - событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию Угрозы Информационной безопасности

Риск нарушения информационной безопасности - Риск, связанный с Угрозой Информационной безопасности.

Обработка риска нарушения информационной безопасности - процесс выбора и осуществления Защитных мер, снижающих Риск нарушения Информационной безопасности, или мер по переносу, принятию или уходу от Риска.

1.2. Правила информационной безопасности при работе в системе дистанционного банковского обслуживания (далее Правила) составлены в соответствии с требованиями Законодательства Российской Федерации, СТАНДАРТОМ БАНКА РОССИИ СТО БР ИББС-1.0-2014 «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ» и другими нормативными документами Банка России, Международными стандартами ISO 27001:2005 и ISO 17799:2005, а также Политикой информационной безопасности АО «СМП-Банк» и являются обязательными к исполнению Клиентами, заключившими Договор ДБО.

1.3. Настоящие Правила определяют Защитные меры по Обработке Рисков нарушения Информационной безопасности при использовании Клиентами Системы ДБО. При этом Клиент обязан учитывать то, что:

- Сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;
- Существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Интернет;
- Существует вероятность атаки Злоумышленников на оборудование, программное обеспечение и информационные ресурсы Клиента, подключенные/доступные из сети Интернет;
- Гарантии по обеспечению Информационной безопасности при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются;
- Меры по нейтрализации Злоумышленных действий могут быть эффективными только в течение первых часов после Инцидента;
- Расследованием Злоумышленных действий и поиском Злоумышленников занимаются правоохранительные органы. В целях проведения расследования пострадавшая сторона должна предоставить в распоряжение следственных органов компьютер, который использовался для доступа в Систему, для проведения экспертизы.

2. Ограничение ответственности Банка

2.1. В связи с тем, что для доступа к услугам дистанционного обслуживания, предоставляемым Банком через Систему ДБО, Клиент использует технические и программные средства, не

принадлежащие Банку, Банк не несет ответственности за любые, в том числе Злоумышленные, действия третьих лиц в отношении и/или с использованием технических и программных средств, когда-либо использовавшихся Клиентом.

2.2. За пользование нелицензированным программным обеспечением Клиент несет уголовную ответственность в соответствии со статьей 146 УК РФ.

2.3. Срок для предъявления Банку претензий по услугам, оказанным с использованием Системы ДБО, составляет 10 календарных дней с даты осуществления операции. По каждой опротестовываемой операции оформляется отдельная претензия. Решение по претензии принимается Банком в течение 30 (тридцати) рабочих дней со дня подачи заявления в офисе Банка и предоставления Клиентом необходимого пакета документов, в соответствии с п. 3.25 настоящих Правил.

2.4. Окончательное решение об использовании предлагаемых Банком в разделе 3 Защитных мер принимает Клиент.

2.5. Банк фиксирует все действия, совершенные от имени Клиента в электронном журнале Системы ДБО. Содержимое журнала Системы ДБО используется при разрешении спорных ситуаций и предоставляется по запросу правоохранительных органов в целях проведения расследования Злоумышленных действий.

3. Защитные меры

3.1. Не сообщайте посторонним лицам, а также кому бы то ни было через сеть Интернет, логины и пароли доступа к ресурсам Банка, историю операций, контактные и учетные данные, так как эти данные могут быть перехвачены Злоумышленником и использованы для получения доступа к Вашим счетам.

3.2. Не записывайте логин и пароль на бумаге, мониторе или клавиатуре.

3.3. Не используйте функцию запоминания логина и пароля в браузерах.

3.4. Не используйте одинаковые логин и пароль для доступа к различным системам.

3.5. Всегда явным образом завершайте сеанс работы с Системой ДБО, используя пункт меню «Выход».

3.6. В случае если доступ к Системе ДБО осуществляется с использованием постороннего компьютера, не рекомендуется сохранять на нем идентификационные данные и другую информацию, а после завершения всех операций нужно убедиться, что идентификационные данные и другая информация не сохранились. После возвращения к штатному персональному компьютеру обязательно смените логин и пароль.

3.7. Если Вы получили на электронную почту письмо с просьбой обновить или предоставить какую-либо информацию со ссылкой на какой-либо сайт или телефон (в том числе – сайт Банка), перезвоните в Службу технической поддержки по телефону (495) 980-24-80 и 8-800-555-2-555 и сообщите о письме или перешлите его на адрес bk@smpbank.ru. Банк никогда не просит передать данные по электронной почте. Обновление данных осуществляется только сотрудником Банка в присутствии представителя Клиента предъявившего документ, удостоверяющего личность. Не открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах и не отвечайте на них.

3.8. Не открывайте приложения к письмам от незнакомых отправителей, так как в них могут быть вирусы (вредоносное программное обеспечение), способные украсть ваши идентификационные данные для входа в Систему ДБО и ключи ЭП.

3.9. Регулярно, не реже одного раза в месяц, производите смену пароля.

3.10. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: ! / { } [ ] < >. Настоятельно рекомендуется использовать специализированные программы-генераторы паролей (пример такой программы размещен по адресу: http://infotecs.ru/products/catalog.php?SECTION_ID=&ID=484).

3.11. Не используйте в качестве пароля имена, памятные даты, номера телефонов.

3.12. Не позволяйте третьим лицам производить за Вас генерацию Криптографических ключей.

3.13. Присоединяйте Ключевой носитель к компьютеру непосредственно перед началом работы с Системой ДБО. По окончании работы извлекайте Ключевой носитель из компьютера.

3.14. Используйте лицензированное программное обеспечение. ПОМНИТЕ: помимо того, что Вы несете уголовную ответственность за пользование нелицензированным программным

обеспечением в соответствии со статьей 146 УК РФ, использование подобного программного обеспечения равноценно предоставлению посторонним лицам доступа на Ваш компьютер.

3.15 Используйте лицензионное, обновляемое не реже одного раза в сутки антивирусное ПО.

3.16. Регулярно (не реже раза в неделю) проводите проверку на наличие новых версий программного обеспечения, установленного на компьютере, производите установку обновлений операционной системы.

3.17. Четко регламентируйте порядок использования компьютера, с которого осуществляется взаимодействие с Системой ДБО, в том числе список лиц и порядок доступа к компьютеру. Не рекомендуется использовать указанный компьютер для доступа к посторонним сайтам.

3.18. Не устанавливайте на компьютере, который используется для взаимодействия с Системой ДБО, постороннее программное обеспечение, например программы автоматического переключения раскладки клавиатуры, различные дополнения к браузерам и т.п. Доказано, что подобные программы передают информацию о содержимом просматриваемых страниц посторонним лицам.

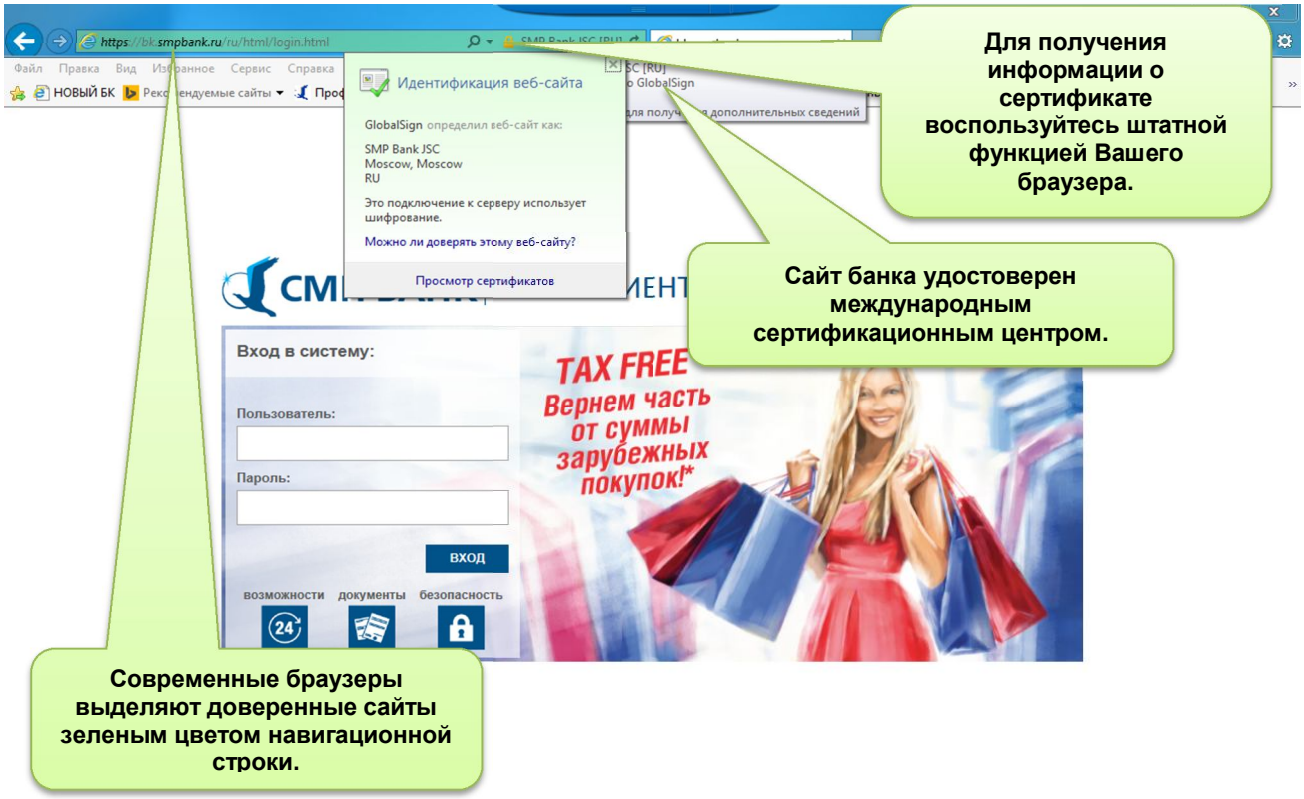
3.19. Не запускайте на своем компьютере программы, полученные из незаслуживающих доверия источников.

3.20. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.

3.21. Настройте браузер на использование протокола защищенной связи TLS. Использование протоколов семейства SSL не обеспечивает надлежащей защиты.

3.22. Не храните незашифрованные идентификационные данные на жестком диске, так как эти данные могут быть похищены Злоумышленником и использованы для получения доступа к Вашим счетам.

3.23. Перед вводом своего логина и пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверьте правильность указания адреса сайта, наличие сертификата безопасности.



В случае обнаружения подозрительных web-сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением официальных сайтов АО "СМП Банк", просьба сообщить об этом по электронной почте bk@smpbank.ru.

3.23. Настройте механизм информирования о входе в Систему ДБО и совершаемых операциях на электронную почту. Регулярно проверяйте почтовый ящик, а также журнал операций

Системы ДБО. Поддерживайте свою контактную информацию в Системе ДБО в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться. В целях оперативного реагирования на Злоумышленные действия пользуйтесь услугой дополнительного информирования.

3.24. В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе, незамедлительно смените логин и пароль, сообщите об Инциденте в Службу технической поддержки и произведите смену Криптографических ключей.

3.25. В случае обнаружения несанкционированных действий со средствами, находящимися на Ваших счетах, необходимо в максимально короткий срок отозвать Сертификат ключа подписи и оформить заявление в операционном подразделении Банка в свободной форме, содержащее максимально подробное описание Инцидента, для инициирования расследования. Для проведения расследования необходимо по согласованию со службой технической поддержки передать в Банк файлы протоколов, подтверждающие установку обновлений операционной системы персонального компьютера и антивирусного программного обеспечения, и в течение 5 (пяти) рабочих дней представить в операционное подразделение Банка для снятия копий документы, подтверждающие факт законного приобретения операционной системы и антивирусного программного обеспечения, а также копию договора об оказании услуг по предоставлению доступа в сеть интернет или иного удостоверяющего факт заключения подобного договора документа (квитанция, чек, счет и тому подобные) и иные документы, которые Клиент сочтет необходимыми для рассмотрения претензии по существу. В случае невозможности представления необходимых файлов и документов об этом делается соответствующая запись на заявлении с указанием причины. Необоснованный отказ в предоставлении требуемых документов может являться основанием для отказа в удовлетворении заявленных Клиентом требований. Решение об обращении в правоохранительные органы Клиент принимает самостоятельно.