ПРАВИЛА
информационной безопасности при использовании систем дистанционного банковского обслуживания через сеть Интернет

1. Общие положения

1.1. Термины и определения

Банк – АО «СМП Банк» (Головной офис, филиалы и внутренние структурные подразделения (дополнительные, операционные и кредитно-кассовые офисы Банка/филиала).

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

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.

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.

Инцидент информационной безопасности (Инцидент) - событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию Угрозы информационной безопасности, т.е. реализацию нарушения свойств информационной безопасности информационных активов Банка. Нарушение может вызываться источниками Угроз информационной безопасности: либо случайными факторами (ошибкой персонала, неправильным функционированием технических средств, природными факторами, например, пожаром или наводнением), либо преднамеренными действиями, приводящими к нарушению доступности, целостности или конфиденциальности информационных активов.

Клиент – физическое лицо (резидент или нерезидент в соответствии с законодательством Российской Федерации), заключившее (заключающее) настоящий Договор, безналичные расчеты которого не связаны с предпринимательской деятельностью.

Обработка риска нарушения информационной безопасности - процесс выбора и реализации защитных мер, снижающих риск нарушения информационной безопасности, или мер по переносу, принятию или уходу от риска.

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

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

Система – система дистанционного банковского обслуживания

Угроза - опасность, предполагающая возможность потерь (ущерба).

Устройство – компьютер, мобильное устройство, планшет, другое средство, с которого осуществляется доступ к Системе.

ЭП – электронная подпись.

1.2. Настоящие Правила информационной безопасности при использовании систем дистанционного банковского обслуживания через сеть Интернет составлены в соответствии с требованиями действующего законодательства Российской Федерации, Положением Банка России «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» от 09.06.2012 №382-П, стандартом Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», Письмом 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" и другими нормативными документами Банка России, Методическими рекомендациями Ассоциации российских банков и НП «Национальный платежный совет» «О порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента», Международными стандартами ISO 27001:2005 и ISO 17799.

1.3. Настоящие Правила определяют рекомендуемые Банком действия Клиентов по Обработке рисков нарушения информационной безопасности при использовании Системы.

1.4. При работе с Системой через сеть Интернет необходимо учитывать следующее:

1.4.1. 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.

1.4.2. Существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Интернет.

1.4.3. Существует вероятность атаки Злоумышленников на оборудование, программное обеспечение и информационные ресурсы, подключенные/доступные к/из сети Интернет.

1.4.4. Гарантии по обеспечению информационной безопасности при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются.

2. Ответственность сторон

2.1. В связи с тем, что для доступа к услугам дистанционного обслуживания, предоставляемым Банком через Систему, 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. Клиент уведомлен о том, что за пользование нелицензированным программным обеспечением Клиент несет уголовную ответственность в соответствии со статьей 146 УК РФ.

2.3. Срок для предъявления претензий по услугам, оказанным с использованием Системы, составляет 10 (Десять) рабочих дней с момента осуществления операции. По каждой опротестовываемой операции оформляется отдельная претензия.

2.4. Окончательное решение об использовании Защитных мер, предлагаемых Банком в разделе 3 настоящих Правил, принимает сам Клиент.

2.5. Банк вправе устанавливать ограничения по составу услуг и объему операций, доступных при использовании той или иной Защитной меры.

2.6. Банк фиксирует все действия, совершенные от имени Клиента в электронном журнале Системы. Содержимое журнала Системы используется при разрешении спорных ситуаций.

3. Рекомендуемые Клиенту Защитные меры

3.1. Не сообщайте посторонним лицам персональные данные или информацию о банковской(ом) карте (Счете) через сеть Интернет, Имена пользователя (логины) и Пароли доступа к ресурсам Банка, историю операций, так как эти данные могут быть перехвачены Злоумышленниками и использованы для получения доступа к Вашим Счетам.

3.2. Не записывайте Имя пользователя (логин) и Пароль на бумаге, мониторе или клавиатуре.

3.3. Не используйте функцию запоминания Имени пользователя (логина) и Пароля в браузерах.

3.4. Не используйте одинаковые Имена пользователя (логин) и Пароль для доступа к различным системам.

3.5. Не пользуйтесь системами, требующими ввода Имени пользователя (логина) и Пароля, на компьютерах, которые находятся в общедоступных местах и в конфигурации которых Вы не уверены. По возможности совершайте операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и (или) информации о Счете.

3.6. Не используйте бесплатный или не защищенный Паролем Wi-Fi для доступа к Системе. Общественные сети не могут гарантировать полную защищенность Ваших данных. Любая информация может быть легко перехвачена Злоумышленниками.

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

3.8. В случае если операция совершается с использованием чужого компьютера, не сохраняйте на нем персональные данные и другую информацию, а после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились (загрузив в браузере иную web-страницу). После возвращения к своему средству доступа обязательно смените Имя пользователя (логин) и Пароль.

3.9. Если Вы получили на электронную почту письмо или получили по иным каналам электронных коммуникаций сообщение с просьбой обновить или подтвердить персональную и любую другую конфиденциальную информацию со ссылкой на какой-либо сайт (в том числе – сайт Банка) перезвоните в Службу клиентской поддержки Банка по телефонам 8 (800) 555-2-555, 8 (495) 980-24-80 и сообщите о письме или перешлите его на адрес ibank@smpbank.ru. **Банк никогда не просит передать данные подобным образом.** Обновление ключевых персональных данных осуществляется только сотрудником Банка и только по обращению Клиента.

Не открывайте ссылки, указанные в сомнительных сообщениях, в которых Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах, и не отвечайте на них.

3.10. Не открывайте приложения к сообщениям от незнакомых отправителей, так как в них может находиться вредоносное программное обеспечение, способное получить доступ к Вашим идентификационным данным и использовать их для входа в Систему.

3.11. При регистрации на сторонних интернет-сайтах всегда изменяйте Пароли, которые приходят Вам по электронной почте. Помните, что Банк никогда не направляет Пароли по электронной почте.

3.12. Регулярно, не реже одного раза в месяц, производите смену Пароля.

3.13. При составлении Пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: ! / { } [ ] < >. Настоятельно рекомендуется использовать специализированные программы-генераторы Паролей (http://www.infotecs.ru/Soft/pass.htm).

3.14. Не используйте в качестве Пароля имена, памятные даты, номера телефонов.

3.15. При использовании ЭП не позволяйте третьим лицам производить за Вас генерацию и ввод ключей.

3.16. Используйте лицензированное программное обеспечение. ПОМНИТЕ: помимо того, что за пользование нелицензированным программным обеспечением предусмотрена уголовная ответственность в соответствии со статьей 146 УК РФ, **использование подобного программного обеспечения равноценно предоставлению посторонним лицам доступа на Ваш компьютер**.

3.17. Регулярно (не реже раза в неделю) проводите проверку на наличие новых версий используемого на Вашем Устройстве, с которого осуществляется доступ к Системе, программного обеспечения и обновляйте

антивирусные базы. В случае обнаружения вредоносного программного обеспечения на компьютере после его удаления незамедлительно смените Имя пользователя (логин) и Пароль в Системе.

3.18. Не запускайте на своем Устройстве, с которого осуществляется доступ к Системе, программы, полученные из незаслуживающих доверия источников.

3.19. Не устанавливайте на Устройство, используемое для работы с Системой, средства удаленного управления, такие как «TeamViewer», «rAdmin» и подобные.

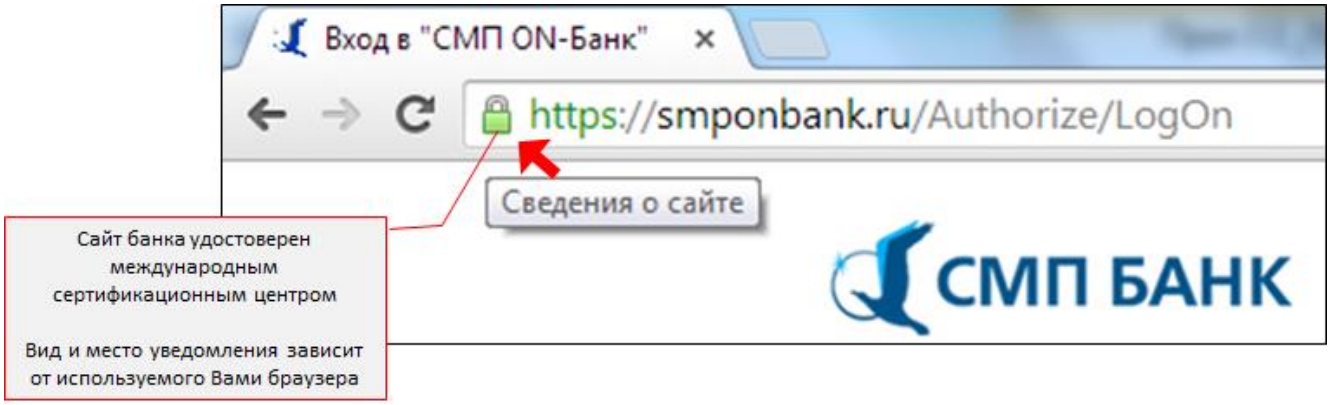
3.20. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.

3.21. Не храните незашифрованные личные данные в электронной почте, «облачных» хранилищах, Устройствах, подключенных к сети Интернет, так как эти данные могут быть похищены Злоумышленниками и использованы для получения доступа к Вашим Счетам.

3.22. Если Вам пришло электронное сообщение о выигрыше в акции, лотерее, розыгрыше удостоверьтесь в его подлинности прежде, чем отсылать деньги на чей-то счет с использованием Системы. Все акции, проводимые Банком не требуют от Клиента перевода денежных средств для получения приза.

3.23. Перед вводом своего Имени пользователя (логина) и Пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверьте правильность указания адреса сайта, наличие сертификата безопасности, и информацию о Вашем последнем доступе в Систему.

Например:



В случае обнаружения подозрительных web-сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением официальных сайтов АО «СМП Банк», сообщите об этом по электронной почте ibank@smpbank.ru.

3.24. Используйте предлагаемые Банком услуги по дополнительному информированию о входе в Систему и совершаемых операциях. Регулярно проверяйте входящую электронную почту, а также контролируйте выписки по Счетам. Поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

3.25. В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе, незамедлительно смените Имя пользователя (логин) и Пароль и сообщите об Инциденте информационной безопасности в Службу технической поддержки Банка. Следуйте указаниям специалистов Банка.

3.26. В случае обнаружения несанкционированных действий со средствами, находящимися на Ваших Счетах, необходимо подать заявление на временное отключение от Системы, подать заявление о преступлении в правоохранительные органы и прекратить использование (обесточить) Устройство, с которого осуществлялся доступ в Систему, в целях сохранения доказательной базы. Если Вы пользуетесь аналогичными Системами других банков – заблокируйте их до выяснения обстоятельств происшествия. Эти учетные записи также могут оказаться скомпрометированными.

3.27. В сети Интернет существует много ресурсов по вопросам информационной безопасности. Регулярно ознакамливайтесь с их содержимым. Помните, Угрозы постоянно видоизменяются и развиваются!

Вам могут быть полезны следующие ресурсы:

«Безопасный интернет»: http://www.saferinternet.ru/

«Управление «К» предупреждает: будьте осторожны и внимательны!»: http://mvd.ru/upload/site1/mvd/mvd2/mvd3/broshyura_k_01_02_20121.pdf

«Вредоносные программы в интернете»: http://mvd.ru/upload/site1/mvd/mvd2/mvd3/liflets_out_1.pdf

«Владельцам пластиковых банковских карт»: http://mvd.ru/upload/site1/mvd1/liflets_out_2.pdf

«Пользователям интернета»: http://mvd.ru/upload/site1/mvd1/liflets_out_3.pdf

«Телефонные мошенники»: http://mvd.ru/upload/site1/mvd1/liflets_out_4.pdf

«Безопасный интернет – детям»: http://mvd.ru/upload/site1/mvd1/liflets_k_deti_06.pdf

«Инструкция по реагированию на инциденты в системах интернет-банкинга»: http://www.group-ib.ru/images/files/Group-IB_dbo_instruction.pdf