Правила информационной безопасности при работе в системе дистанционного банковского обслуживания АКБ «Алмазэргиэнбанк» АО

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, а также Политикой информационной безопасности АКБ «Алмазэргиэнбанк» АО (далее – Банк) и являются обязательными к исполнению Клиентами, заключившими Договор на подключение к системам дистанционного банковского обслуживания (далее – ДБО).

1. Общие положения

1.1. Настоящие Правила являются обязательным **Приложением к «Условиям предоставления услуг с использованием системы дистанционного банковского обслуживания «АЭБ Бизнес».**

1.2. 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.

1.3. Термины и определения, используемые в настоящем документе:

- **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.

2. Ограничение ответственности Банка

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

2.3. 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 никому, в том числе сотрудникам банка, логины и пароли доступа к ресурсам Банка. Не сообщайте посторонним лицам, в том числе через сеть интернет, историю операций, контактные и учетные данные, так как эти данные могут быть использованы Злоумышленниками для получения доступа к Вашим счетам.

3.2. Не записывайте логин и пароль и не храните их в местах где к ним могут получить доступ посторонние люди.

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, используя пункт меню «Выход».

3.6. Не рекомендуется использовать чужой компьютер для доступа к Системе ДБО, в случае если доступ к Системе ДБО необходимо осуществить 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 Банка и сообщите о письме. Банк никогда не просит передать данные для входа в ДБО. 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 и ключи ЭП.
3.9. Регулярно, 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.
3.11. Не используйте в качестве пароля имена, памятные даты, номера телефонов.
3.12. Не позволяйте третьим лицам производить за Вас генерацию ключей ЭП.
3.13. Присоединяйте ключевой носитель ЭП 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. Регулярно (не реже раза в неделю) проводите проверку на наличие обновлений операционной системы и программного обеспечения, установленного на компьютере, и обновляйте антивирусные базы. В случае обнаружения вирусов (вредоносного программного обеспечения) на компьютере, после его удаления незамедлительно смените логин и пароль в Системе и произведите замену ключей ЭП.
3.16. Четко регламентируйте порядок использования компьютера, с которого осуществляется взаимодействие с Системой, в том числе список лиц и порядок доступа к компьютеру. Не рекомендуется использовать указанный компьютер для доступа к посторонним сайтам.
3.17. Не устанавливайте на компьютере, который используется для взаимодействия с Системой, 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.
3.18. Не запускайте на своем компьютере программы, полученные из незаслуживающих доверияисточников.
3.19. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.
3.20. Настройте браузер на использование протокола защищенной связи TLS. Использование протоколов семейства SSL не обеспечивает надлежащей защиты.
3.21. Не храните незашифрованные идентификационные данные на жестком диске, так как эти данные могут быть похищены Злоумышленником и использованы для получения доступа к Вашим счетам.
3.22. 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 официального сайта АКБ «Алмазэргиэнбанк» АО, просьба сообщить об этом по электронной почте sib@albank.ru.
3.23. Настройте механизм информирования о входе в Систему и совершаемых операциях на электронную почту или СМС. Регулярно проверяйте входящие сообщения, а также журнал операций Системы. Поддерживайте свою контактную информацию в Системе в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.
3.24. Не передавайте мобильное устройство третьим лицам, а также храните в недоступном для третьих лиц месте мобильное устройство, на которое поступают СМС-сообщения на ваш мобильный номер оператора связи для подтверждения операций в Системе.
3.25. Не устанавливайте непроверенные мобильные приложения, в частности с неизвестных источников, на мобильное устройство, на которое поступают СМС-сообщения на ваш мобильный номер оператора связи для подтверждения операций в Системе.

3.26. Установите антивирусное приложение на мобильное устройство, на которое поступают СМС-сообщения на ваш мобильный номер оператора связи для подтверждения операций в Системе.

3.27. Обязательно уведомляйте Банк перед сменой номера мобильного оператора связи, на которое поступают СМС-сообщения для подтверждения операций в Системе.

3.28. 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 ключей ЭП.

3.29. В случае обнаружения несанкционированных действий со средствами, находящимися на Ваших счетах, необходимо в максимально короткий срок отозвать сертификат ЭП и оформить заявление на имя Председателя Правления Банка в свободной форме, содержащее максимально подробное описание инцидента, для инициирования расследования. Для проведения расследования необходимо по согласованию со службой информационной безопасности 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 Службу информационной безопасности 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.

Приложения

1. «Памятка для клиентов о действиях в случае обнаружения несанкционированного списания»

Дополнение к Приложению № 3
к «Правилам информационной безопасности
при работе в системе дистанционного
банковского обслуживания «АЭБ Бизнес»

ПАМЯТКА ДЛЯ КЛИЕНТОВ
о действиях в случае обнаружения несанкционированного списания

В случае обнаружения несанкционированного списания со счета Банк рекомендует Клиенту осуществить следующие действия:

1. Максимально оперативно представить письменное заявление в Банк, заверенное печатью и подписью руководителя, по возможности, на бланке организации о факте несанкционированного списания с указанием даты, суммы платежа, других известных Клиенту обстоятельств, а также с просьбой об оказании содействия в возврате несанкционированно списанных денежных средств. Указанное заявление необходимо представить в Банк на бумажном носителе в срок не позднее 2-х рабочих дней с даты устного обращения в Банк.

2. Не использовать компьютеры, которые эксплуатировались для работы в Системе. Их необходимо отключить от сети. С высокой долей вероятности они заражены специализированным вредоносным программным обеспечением, поэтому этот шаг позволит предотвратить последующие инциденты, а также сохранить доказательства для проведения технической экспертизы.

3. Произвести смену ключей шифрования и ключей ЭП, используемых для работы с Системой в соответствии с действующим Договором. **До момента смены ключей работа в Системе будет прекращена в связи с компрометацией действующих средств доступа.**

4. В случае подтверждения операций СМС-сообщениями – заблокируйте мобильное устройство и вытащите SIM-карту, а также попросите выписку СМС-сообщений у мобильного оператора связи и заблокируйте SIM-карту, предварительно уведомив Банк.

5. По факту несанкционированного доступа к компьютерной информации обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по статьям 272 и 273 УК РФ в связи с созданием, использованием и распространением неустановленными лицами вредоносных компьютерных программ, повлекшим неправомерный доступ неустановленных лиц к Вашей компьютерной информации, что, в свою очередь, привело к несанкционированному Клиентом переводу денежных средств Клиента.

6. С копией указанного заявления с приложением копии талона правоохранительного органа о приеме заявления, обратиться в Арбитражный суд с исковым заявлением в отношение банка-получателя о возврате неосновательного обогащения с ходатайством об аресте похищенной суммы денежных средств на счете получателя в банке получателя и раскрытии персональных данных получателя в целях привлечения его в качестве соответчика (гл. 60 ГК РФ) Если известны полные реквизиты получателя – физического лица, указанный иск подается в суд общей юрисдикции.

7. Копии вышеуказанных обращений в правоохранительные органы и суд с отметками о приеме необходимо предоставить в Банк для того, чтобы Банк мог оказать содействие в возврате несанкционированно списанных средств.

Указанные действия произвести в течение 2-х рабочих дней с даты обнаружения несанкционированного списания в целях оперативного противодействия дальнейшему переводу и обналичиванию денежных средств.