Правила информационной безопасности при работе в системе дистанционного банковского обслуживания (Эсхата Бизнес) ОАО «Банк Эсхата»

Правила информационной безопасности при работе в системе дистанционного банковского обслуживания (далее – Правила) составлены в соответствии с требованиями Законодательства РТ, и другими нормативными документами НБТ, а также Политикой информационной безопасности ОАО «Банк Эсхата» (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 «Эсхата 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. Ответственности сторон

2.1. Обязанности Банка:

- Банк обязуется обеспечить доступность Службы поддержки клиентов Банка (808) для взаимодействия с Клиентами по вопросам предоставления услуг через удаленные каналы обслуживания.
- Банк обязуется предоставить услуги по обслуживанию Клиентов своевременно (сброс пароля, регистрация Клиента) в течении рабочего дня.

2.2. Обязанности клиента:

- Клиент обязан за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые для обмена документами по Системе ДБО.
- Клиент обязуется сохранять в тайне применяемую в Системе ДБО Ключевую информацию.
- Клиент обязуется ознакомиться с мерами безопасности при работе в Системе ДБО, и неукоснительно их соблюдать.
- Клиент соглашается с получением услуг посредством Системы ДБО через сеть Интернет, осознавая, что сеть Интернет не является безопасным каналом связи, и соглашается нести финансовые риски и риски нарушения конфиденциальности, связанные с возможной компрометацией информации при её передаче через сеть Интернет.

2.3. 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.
- за сбои в работе электронной почты, сети Интернет, сетей связи, возникшие по не зависящим от Банка причинам и повлекшие за собой несвоевременное получение или неполучение Клиентом уведомлений Банка.
- в случае, если информация Клиента (логин/пароль от Системы ДБО), станет известной иным лицам в результате недобросовестного выполнения Клиентом условий их хранения и использования.
- за ненадлежащее исполнение своих обязательств по ДБО в случае, если исполнение оказалось невозможным вследствие обстоятельств непреодолимой силы (т.е. чрезвычайных, непредотвратимых при данных условиях обстоятельств). К таким обстоятельствам относятся, в частности, пожары, стихийные бедствия (землетрясения, наводнение, ураган), массовые заболевания (эпидемии), забастовки, военные действия, террористические акты, диверсии, запрет операций, в том числе с отдельными странами, вследствие принятия международных санкций и другие, не зависящие от воли сторон обстоятельства.
- в случаях невыполнения Клиентом условий ДБО.
- за ущерб и факт разглашения банковской тайны, возникшие вследствие допуска Клиентом третьих лиц к использованию мобильного устройства, номер которого зарегистрирован Клиентом для доступа к Системе ДБО.
- за ущерб, возникший в результате несвоевременного уведомления Банка о прекращении использования номера мобильного телефона.
- 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 при работе в системе ДБО

Банк информирует Клиентов о мерах безопасности при работе в Системе ДБО, рисках Клиента и возможных последствиях для Клиента в случае несоблюдения им мер информационной безопасности, рекомендованных Банком. Информирование осуществляется на сайте Банка или в Подразделениях Банка, или путем отправки SMS-сообщений на номер мобильного устройства

Клиента, зарегистрированный для доступа к Системе ДБО, или иными способами, установленным в ДБО.

3.1. Обеспечение безопасности ключевой информации.

- Не сообщайте никому, в том числе сотрудникам банка, логины, пароли доступа, одноразовые пароли 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.
- Храните в недоступном для третьих лиц месте свои аутентификационные данные.
- При Компрометации или подозрении на Компрометацию пароля доступа – незамедлительно произвести смену пароля в настройках Системы ДБО. При невозможности незамедлительно выполнить указанные выше действия, незамедлительно обратиться в Службу поддержки Банка или любое Подразделение Банка.
- Не используйте одинаковые логин и пароль для доступа к различным системам.
- Регулярно, производите смену Пароля. Пароль должен содержать не менее 10 знаков. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: /; *; -; +; @; &. Настоятельно рекомендуется использовать специализированные программы-генераторы паролей.
- Не используйте в качестве пароля имена, памятные даты, номера телефонов.
- Не храните незашифрованные идентификационные данные на жестком диске, так как эти данные могут быть похищены Злоумышленником и использованы для получения доступа к Вашим счетам.

3.2. Соблюдение общих правил безопасного использования системы дбо.

- 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.
- Всегда явным образом завершайте сеанс работы с Системой ДБО, используя пункт меню «Выход».
- 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.
- Отключить функцию «Общие файлы», при использовании компьютера в локальной рабочей сети.
- Настройте механизм информирования о входе в Систему и совершаемых операциях на СМС уведомления. 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.
- В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе ДБО, незамедлительно смените логин и пароль, сообщите об инциденте в Службу поддержки клиентов Банка и произведите смену ключей ЭЦП.

3.3. Соблюдение правил безопасного использования эцп.

При использовании ключа ЭЦП соблюдайте следующие правила:

- Не передавайте ключевой носитель третьим лицам, не оставляйте его без присмотра, не храните в доступном месте.
- При получении ключевого носителя создайте резервную копию, хранимую в сейфе.
- На электронном носителе, на котором расположены ключи, не должно быть другой информации.
- Хранение ключа ЭЦП на жестком диске недопустимо.
- Не позволяйте третьим лицам производить за Вас генерацию ключей ЭЦП.

- Присоединяйте ключевой носитель ЭЦП к компьютеру непосредственно перед началом работы с Системой ДБО. По окончании работы извлекайте ключевой носитель из компьютера.
- Незамедлительно проводить замену сертификата проверки ключа ЭЦП при смене должностных лиц, наделенных полномочиями по распоряжению денежными средствами на расчетном счете юридического лица.

3.4. Использование и обновление системного и прикладного по.

- Использовать и оперативно обновлять лицензионное системное и прикладное программное обеспечение (ПО) только из доверенных источников, гарантирующих отсутствие вредоносных программ.
- Использовать и оперативно обновлять специализированное ПО для защиты информации - антивирусное ПО. Выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ. В случае обнаружения вирусов (вредоносного программного обеспечения) на компьютере, после его удаления незамедлительно смените логин и пароль в Системе и произведите замену ключей ЭЦП.
- 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.
- Не запускайте на своем компьютере программы, полученные из незаслуживающих доверия источников. В случае установки на компьютеры, на которых ведется работа в системе ДБО, программ для удаленной поддержки пользователей (например, TeamViewer, AnyDesk и т.п.), Клиент полностью принимает на себя все риски настроек безопасности доступа в этих программах, передачи третьим лицам.

3.5. Соблюдение правил безопасной работы в сети интернет.

- Не осуществлять вход в Систему ДБО и проведение операций в Системе ДБО с использованием не доверенных (публичных) беспроводных сетей.
- Не используйте функцию запоминания логина и пароля в браузерах.
- 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.
- 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 ЭЦП.
- Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.
- Настройте браузер на использование протокола защищенной связи TLS. Использование протоколов семейства SSL не обеспечивает надлежащей защиты.
- 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 ОАО «Банк Эсхата», просьба сообщить об этом по телефону 808 или по электронной почте chatcenter@eskhata.tj.

3.6. Соблюдение правил при работе с мобильными устройствами.

- Клиент обязан исключить возможность использования третьими лицами номера мобильного устройства, зарегистрированного для доступа к Системе ДБО. Установите на телефоне/смартфоне пароль для доступа к устройству, данная возможность доступна для любых современных моделей телефонов/смартфонов.

- При потере или краже мобильного устройства, на котором установлено ПО «Google authenticator» для подтверждения электронных операции, необходимо незамедлительно сообщить в Службы поддержки клиентов Банка (808). Только после этого доступ к Системе ДБО будет заблокирован, и злоумышленник не сможет воспользоваться вашим Счетом в Банке.
- Не устанавливайте непроверенные мобильные приложения, в частности с неизвестных источников, на мобильное устройство, на которое установлено ПО «Google authenticator» для подтверждения операций в Системе.
- Установите антивирусное приложение на мобильное устройство, на которое установлено ПО «Google authenticator» для подтверждения операций в Системе.

Клиент обязан информировать Банк о прекращении использования номера мобильного телефона, зарегистрированного для доступа к Системе ДБО, а также о следующих факторах:

- о факте смены абонентского номера Клиента;
- о факте расторжения с оператором связи договора об оказании Клиенту услуг связи по инициативе Клиента;
- о факте наличия вредоносного программного обеспечения на Мобильном устройстве Клиента;
- о факте смены Мобильного устройства Клиента;
- о факте подключенной услуги переадресации вызова и сообщений к абонентскому номеру Клиента.