Правила информационной безопасности при работе в приложении «Эсхата Онлайн»

Правила информационной безопасности при работе в приложении Эсхате Онлайн (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 Эсхата Онлайн (далее – ЭО).

1. Общие положения

1.1. Настоящие Правила являются обязательным Приложением к «Условиям предоставления услуг с использованием «Эсхата Онлайн».

1.2. Настоящие Правила определяют Защитные меры по обработке Рисков нарушения Информационной безопасности при использовании Клиентами Системы ЭО.

1.3. Средства и методы защиты информации, применяемые в Банке, позволяют обеспечить необходимый уровень безопасности при осуществлении переводов денежных средств и предотвратить мошеннический вывод денежных средств со счетов клиентов при условии выполнения клиентами рекомендаций, изложенных в данном документе.

1.4. Термины и определения:

- **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.
- **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.
- **Клиент** – физическое лицо, которое пользуется услугами Банка.
- **Мобильное устройство** - электронное устройство (планшет, смартфон, мобильный телефон и т.п.), находящееся в личном пользовании Клиента, имеющее подключение к мобильной (подвижной радиотелефонной) связи и/или информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет)
- **Антивирусная защита** - специализированное программное обеспечение, предназначенное для обнаружения, блокировки и удаления вирусов, вредоносных программ и других угроз безопасности, которые могут заражать мобильные устройства.
- **Защита от фишинга** - меры и технологии, направленные на предотвращение атак, когда злоумышленники пытаются обмануть пользователей, выдавая себя за доверенные организации или лица с целью получения конфиденциальной информации, такой как логины, пароли, номера кредитных карт и другие личные данные.

2. Ответственность сторон

2.1. Банк обязуется:

- Не разглашать и не передавать третьим лицам информацию о Клиенте и его операциях в системе ЭО, за исключением случаев, предусмотренных действующим законодательством Республики Таджикистан
- Обеспечивать информационную безопасность ЭО в соответствии с требованиями законодательства РТ.
- Банк обязуется обеспечить доступность Службы поддержки клиентов Банка (808) для взаимодействия с Клиентами по вопросам предоставления услуг через удаленные каналы обслуживания.
- Банк информирует Клиента о мерах безопасности, рисках Клиента и возможных последствиях для Клиента в случае несоблюдения мер информационной безопасности, рекомендованных Банком. Информирование осуществляется также на Официальном сайте Банка и/или в Подразделениях Банка и/или путем отправки SMS-сообщений.

2.2. Клиент обязуется:

- Клиент самостоятельно и за свой счет обеспечивает подключение своих устройств к сети Интернет, а также обеспечивает защиту собственных устройств от несанкционированного доступа и вредоносного программного обеспечения. В случае использовании ЭО на не принадлежащих Клиенту устройствах, Клиент соглашается нести все риски, связанные с возможным нарушением конфиденциальности и целостности информации, а также возможными неправомерными действиями иных лиц.
- Клиент обязуется ознакомиться с мерами безопасности при работе в ЭО, и неукоснительно их соблюдать.

2.3. Банк не несет ответственности:

- 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 и Отчетов по Карте/ Выписок/Справок.
- если информация о пароле «Эсхата Онлайн», станет известной иным лицам в результате недобросовестного выполнения Клиентом условий их хранения и использования.
- за ненадлежащее исполнение своих обязательств по ЭО 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.
- за ущерб и факт разглашения банковской тайны, возникшие вследствие допуска Клиентом третьих лиц к использованию мобильного устройства, номер которого зарегистрирован Клиентом для доступа к ЭО.
- за ущерб, возникший вследствие утраты или передачи Клиентом Мобильного устройства неуполномоченным лицам

3. Защитные меры при использовании ЭО

Банк информирует Клиентов о мерах безопасности при работе в ЭО, рисках Клиента и возможных последствиях для Клиента в случае несоблюдения им мер информационной безопасности, рекомендованных Банком.

3.1. Обеспечение безопасности ключевой информации.

Не передавайте посторонним лицам одноразовые пароли, PIN-коды и SMS-коды подтверждения операций.

Не используйте одинаковый пароль для доступа к различным системам.

Избегайте использования в паролях дат, имён, номеров телефонов и другой персональной информации, которая может быть угадана или найдена в открытых источниках.

Избегайте хранения паролей в открытом виде. Не записывайте пароли на бумажных листках (или в текстовых файлах на устройствах), не оставляйте их в легкодоступных местах (на рабочем столе), не передавайте их неуполномоченным лицам. Для хранения паролей используйте менеджер паролей.

3.2. Соблюдение правил безопасной работы в сети интернет.

Клиент соглашается с получением услуг посредством ЭО 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.

Используйте только надежные и проверенные точки Wi-Fi. Не рекомендуется подключаться к популярным и/или бесплатным точкам доступа Wi-FI, если Вы не уверены в достоверности имени точки доступа, а также отключайте Wi-Fi и Bluetooth, если в данный момент они не используются.

Будьте осторожным при открытии электронных писем или переходе по ссылкам, особенно если они запрашивают вашу личную информацию или логин и пароль от электронного кошелька.

3.3. Соблюдение правил при работе с мобильными устройствами.

Регулярно обновлять приложение до последней версии.

В случае изменения номера мобильного телефона для работы в ЭО, необходимо обратиться в ближайший центр обслуживания Банка или при помощи приложения ЭО для идентификации нового номера. Необходимо помнить, что старый номер мобильный оператор может передать другому абоненту в случае, если он неактивен некоторое время.

Клиент обязан исключить возможность использования третьими лицами номера мобильного телефона, зарегистрированного для доступа к ЭО.

Установите на мобильное устройство лицензионное антивирусное программное обеспечение, обеспечьте автоматическое обновление антивирусных баз.

Для доступа к мобильному устройству установите пароль и настройте автоматическую блокировку устройства.

Загружайте и устанавливайте программное обеспечение только из проверенных и надежных источников – Google Play или App Store.

Производите своевременное обновление системы и используемых программ.

Удаляйте конфиденциальную информацию в случае передачи мобильного устройства другим лицам (продажа устройства, передача в ремонт). Воспользуйтесь функцией восстановления заводских настроек.

В случае обнаружения подозрительных действий, совершенных с Вашего кошелька, незамедлительно сообщите об инциденте в Службу технической поддержки.