Приложение 2
«OnlineSecurity»
Инструкция пользователя

1. ОБЩИЕ СВЕДЕНИЯ

1. Термины

Специальные термины, используемые в настоящем Приложении, приведены в таблице ниже.

Термины	Определения
QR-код	Способ входа в систему. Код — система условных знаков для представления информации.

2. **Проверка на наличие подключения ЕШДИ перед приобретением Услуги:**

Единый шлюз доступа к Интернету (ЕШДИ) – аппаратно-программный комплекс, предназначенный для защиты сетей телекоммуникаций при доступе к Интернету и (или) сетям связи, имеющим выход в Интернет.

У компаний с ЕШДИ защитой нет доступа к OnlineBank через защищенный рабочий стол OnlineSecurity, поэтому перед подключением услуги, необходимо убедиться в отсутствии ЕШДИ защиты.

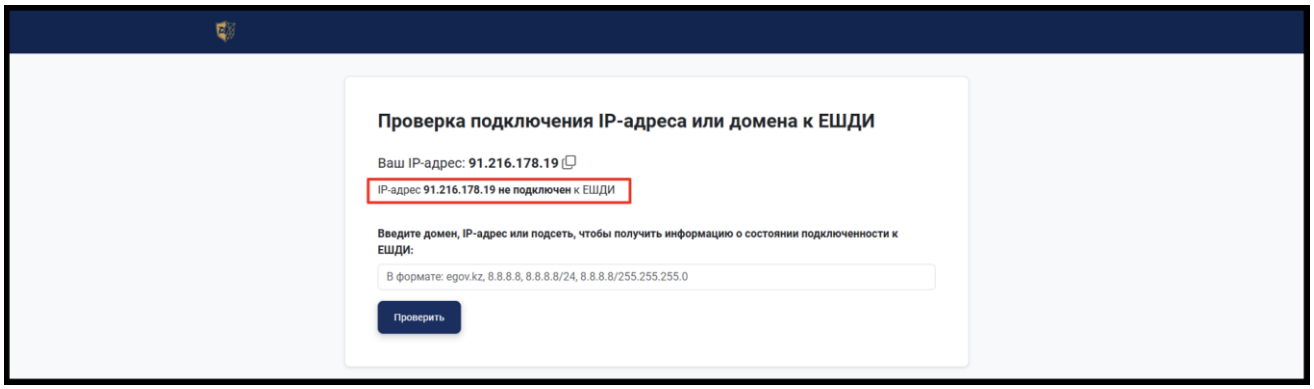
Инструкция для самостоятельной проверки клиента

Шаг 1. Перейти по ссылке https://checkip.sts.kz/

Откроется портал ЕШДИ, автоматически определяющий IP пользователя и наличие ЕШДИ защиты, или ее отсутствие.

Шаг 2. Выявить, подключен ЕШДИ или нет

В поле, отмеченном красным, будет написано – «подключен к ЕШДИ» или «не подключен к ЕШДИ». Сообщите менеджеру, какой ответ выходит у вас.



«подключен к ЕШДИ» - подключение к услуге OnlineSecurity НЕВОЗМОЖНО

«не подключен к ЕШДИ» - подключение к услуге OnlineSecurity ВОЗМОЖНО

Инструкция для проверки менеджером техподдержки

Шаг 1. Получить рабочий IP пользователя

Стандартный процесс определения IP на Windows (клиент должен выполнить эти операции у себя):

1. Откройте командную строку:

Нажмите клавиши Win + R, введите cmd и нажмите Enter.

2. Введите команду ipconfig:

Напечатайте ipconfig и нажмите Enter.

3. Найдите IP-адрес:

В результатах поиска найдите раздел, соответствующий вашему типу подключения (например, ""Адаптер беспроводной локальной сети Беспроводная сеть"" для Wi-Fi или ""Адаптер Ethernet"" для проводного подключения).

4. Найдите IPv4-адрес:

Внутри этого раздела найдите строку ""IPv4-адрес"". Значение рядом с этой строкой и будет вашим IP-адресом.

Если стандартный процесс не помог с определением IP, можно попробовать альтернативные способы (использовать Google), или попросить помощи у системного администратора в компании клиента.

Шаг 2. Перейти по ссылке https://checkip.sts.kz/

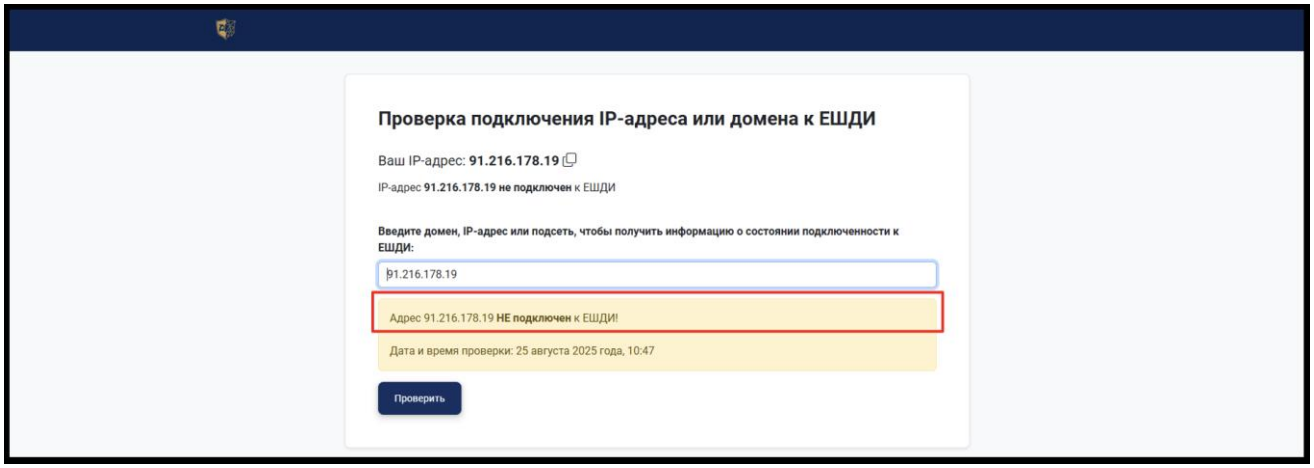
Откроется портал ЕШДИ.

Шаг 3. Прописать IP клиента

Определенный ранее IP ввести в портал

Шаг 4. Выявить, подключен ЕШДИ или нет

В ответе, отмеченном красным, будет написано – «подключен к ЕШДИ» или «не подключен к ЕШДИ».



«подключен к ЕШДИ» - подключение к услуге OnlineSecurity НЕВОЗМОЖНО

«не подключен к ЕШДИ» - подключение к услуге OnlineSecurity ВОЗМОЖНО"

3. Порядок авторизации в систему Onlinebank после приобретения Услуги:

По завершению подключения Услуги согласно приложению «Инструкция подключения», Заказчик подключается к системе Onlinebank только при использовании Услуги:

3 .1. Предоставлен способ авторизации в Услугу посредством QR-кода в мобильном приложении Onlinebank.

Внимание: после приобретения Услуги, Заказчик подключается к системе Onlinebank только с помощью использования Услуги.

4. Общий порядок действий пользователя при работе с Услугой

По завершению подключения Услуги согласно приложению «Инструкция подключения», Заказчик может выполнять следующие действия для работы с Услугой:

4 .1. Изменение тарифа

4 .1.1. Во время действия Услуги Заказчик может поменять количество пользователей Услуги, которое повлияет на текущий тариф.

4 .1.2. Для этого Заказчик подключается к системе Onlinebank, переходит в личный кабинет и выбирает вкладку «Защищенный кабинет бухгалтера», где предоставлена информация по текущему тарифу Заказчика, при нажатии кнопки «Сменить тариф», Заказчик получит доступ к тарифной сетке и может выбрать новый тариф.

4 .1.3. После смены тарифа Заказчику будет направлено уведомление об успешной смене тарифа. Данные по новому тарифу будут отображены в Личном кабинете в системе Onlinebank.

4 .2. Отказ от услуги

4 .2.1. Процесс отмены Услуги происходит в личном кабинете системы Onlinebank, во вкладке «Защищенный кабинет бухгалтера».

4 .2.2. Заказчику предоставлена информация по текущему тарифу, его стоимости и сроке действия. Заказчик может выбрать отказаться от услуги, путем нажатия кнопки «Отключить». Далее заказчику необходимо нажать «Подтвердить», для подтверждения отказа от услуги.

4 .2.3 Заказчик переходит по ссылке на инструкцию по отключению от Услуги на сайт Kazteleport.kz. Клиент скачивает, заполняет с печатью компании и высылает заполненное «Приложение 2» к договору присоединения по адресу contact@kazteleport.kz с темой: OnlineSecurity. «Отключение от услуги», либо нарочно, по-адресу: г. Алматы, ул. Абая 109в.

4 .3. Импорт и экспорт файлов из системы Onlinebank

4 .3.1. При использовании Onlinebank Заказчик имеет возможность экспортировать и импортировать файлы из локальной папки на личном рабочем столе.

4 .3.2 Локальный профайл пользователя с его файлами (по умолчанию C:/Users/{username}) подключается к «Защищенному кабинету бухгалтера».

4 .3.3 Клиент вправе добавить в программе Horizon любую доступную Клиенту локальную или сетевую папку, необходимую для подключения к «Защищенному подключения бухгалтера»

5. Общие сведения по обращению в техническую поддержку в случае возникновения вопросов работы с Услугой

5 .1. В случае возникновения проблем с Услугой Заказчик обращается к службе поддержки системы Onlinebank.

6. Общие правила информационной безопасности со стороны Заказчика

6 .1. Заказчик несет ответственность за обеспечение информационной безопасности в своей корпоративной инфраструктуре. Обеспечение информационной безопасности может включать, но не ограничивается, следующими пунктами:

- Применение Заказчиком лицензированного ПО;
- Применение Заказчиком антивирусного решения на корпоративных рабочих стронциях, применяющихся для подключения к Услуге;
- Наличие ширины интернет канала - 5 Мбит/сек и более;
- Применение лицензионной операционной системы Microsoft Windows 10 (x64) Version 21H2, Enterprise LTSC 2019 и выше, Windows 11 (x64) Version 22H2 и выше, Windows Server с последними обновлениями 2016, 2019, Mac OS Monterey (12) и выше (с официальной лицензией, и установленными обновлениями до последней/актуальной версии), Ubuntu 24.04/22.04/20.04;
- Применять рекомендации по настройкам безопасности в операционной системе Microsoft Windows 10 и выше;
- Заказчик осуществляет действия по обеспечению безопасности собственного доступа в сеть Интернет;
- Превентивные меры по повышению осведомленности пользователей Заказчика, непосредственно взаимодействующих с Услугой, в области атак социальной инженерии;
- Ограничить установку и использование программ, позволяющих получить удаленный доступ к компьютеру такие, как Team Viewer, RAdmin и т.д на рабочих станциях, применяемых для подключения к Услуге;
- Наличие пароля на мобильных устройствах Заказчика;
- Отсутствие на рабочих станциях таймера блокировки компьютера;

6 .2. Клиент обязуется исполнять рекомендации Банка в части обеспечения безопасности, включая, но не ограничиваясь перечнем мер в настоящем пункте, на устройствах, с помощью которых осуществляется работа с Системой Onlinebank (Мобильное устройство и/или Рабочая станция):

- не устанавливать на свое устройство, с которого выполняется вход в Систему Onlinebank, программы для удаленного администрирования (прим. TeamViewer, AmmyyAdmin, AnyDesk, RustDesk и т.д.);
- никогда не заходить на сайт Системы Onlinebank по ссылкам, указанным в электронных письмах, не открывать файлы, полученные из ненадежных источников через сети интернет или через съемные носители, без проведения предварительной проверки на предмет содержания в них вирусов, плагинов или вредоносных программ;
- не оставлять без контроля компьютер при включенном питании, загруженном программном обеспечении и подключенные к Рабочей станции Ключевые носители;
- при завершении работы с Системой Onlinebank обязательно осуществлять выход, нажав на кнопку «Выход»;

6 .3. Исполнитель не несет ответственность за обеспечение информационной безопасности в инфраструктуре Заказчика. В случае возникновения инцидента информационной безопасности на стороне Заказчика, Исполнитель не несет ответственности за любые

задержки, прерывания, прямой ущерб или упущенную выгоду и потери со стороны Заказчика. В случае если Заказчик считает, что инцидент информационной безопасности произошел по вине Исполнителя, Заказчик обязан предоставить доказательства исполнителю.

6 .4. При получении доступа к Системе Onlinebank посредством Мобильного приложения Клиент должен обеспечить самостоятельное наличие мобильного устройства, отвечающего следующим параметрам:

- версия мобильной ОС не ниже Android 5.X и iOS 13.0;
- с минимальным размером экрана не меньше 800 x 480 (hdpi) для устройств на базе мобильной ОС Android;
- доступ в интернет.

6 .5. Клиент обязуется незамедлительно обратиться по доступным каналам связи к Исполнителю при выявлении каких-либо аномалий, затемнение экранов, потеря контроля управления Рабочей станции прервать работу на компьютере, отключить его от питания.

6 .6. При использовании Мобильного устройства для работы с Мобильным приложением Onlinebank Клиент обязуется руководствоваться следующими правилами и рекомендациями по безопасности:

- при работе с Мобильным приложением Onlinebank, обязательно установить в настройках блокировку Мобильного устройства (PIN-код, пароль, графический ключ или биометрические данные TouchID/FaceID), а также установить автоматическую блокировку Мобильного устройства;
- Устанавливать приложения и их обновления только через официальные магазины: Google Play, Apple Store, AppGallery. Установка приложений из сторонних источников запрещена;
- не использовать взломанные Мобильные устройства с активированными правами супер-пользователя (root для операционной системы Мобильного устройства на Android, или jailbreak для операционной системы Мобильного устройства на iOS);
- не открывать ссылки и SMS сообщения на Мобильном устройстве, полученные от неизвестных лиц;
- не хранить на Мобильном устройстве конфиденциальную информацию, PIN-коды от банковских платежных карточек, PIN-код от ключевых носителей;
- незамедлительно производить блокировку SIM-карты в случае утери или кражи Мобильного устройства, обратившись к оператору, а также произвести блокировку пользователя Системы Onlinebank, обратившись в Контакт-центр системы Onlinebank.