ПРИЛОЖЕНИЕ 2

«ЗАЩИЩЕННЫЙ ВИРТУАЛЬНЫЙ КАБИНЕТ БУХГАЛТЕРА»

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. 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:

2.1. 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.

3. 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:

3.1. Изменение тарифа

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

3.1.2. 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.

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

3.2. Отказ от услуги

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

3.2.2. 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.

3.2.3 После подтверждения об отказе от Услуги, Заказчик заходит в систему Onlinebank через обычное подключение интернет не включающую Услугу.

3.3. Импорт и экспорт файлов из системы Onlinebank

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

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

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

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

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

5. Общие правила информационной безопасности со стороны Заказчика

5.1. 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;
- Применение лицензионной операционной системы Microsoft Windows 10 и выше, Mac OS последней версии (с официальной лицензией, и установленными обновлениями до последней/актуальной версии);
- 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;

5.2. 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»;

5.3. 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.

5.4. 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.

5.5. 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.

5.6. 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.