UniCredit Bank
Joint Stock Company
9, Prechistenskaya emb., Moscow, Russia, 119034

ЮниКредит Банк
Акционерное общество
Россия, Москва, 119034, Пречистенская наб., 9

УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

При использовании системы Business.Online и технологии Host-to-Host в качестве электронных средств платежа (далее – электронный документооборот) клиент несет повышенные риски нарушения конфиденциальности и несанкционированного списания средств с его счетов неуполномоченными лицами, в том числе при компрометации ключей электронной подписи и/или носителей одноразовых паролей, а также при несанкционированном удаленном управлении системой, в том числе с использованием вредоносного кода.

Использование клиентом электронного документооборота является подтверждением приемлемости для него указанных рисков.

В целях снижения указанных рисков использования электронного документооборота с Банком применяются следующие средства защиты:

Система Business.Online	Технология Host-to-Host
• **SSL шифрование данных** - криптографический протокол, обеспечивающий безопасное соединение между веб-браузером и сервером системы. • **Сертификат безопасности сайта** - веб-портал системы имеет сертификат безопасности, выданный Интернет центром сертификации. Благодаря указанному сертификату браузер пользователя имеет возможность проверить подлинность сайт системы. При некорректном сертификате браузер ограничивает вход на такой сайт и отображается соответствующее предупреждение. • **Использование одноразовых паролей** - для отправки сообщения в Банк необходимо дополнительное подтверждение с помощью одноразовых паролей. • **Автоматический выход из системы** - если в течение 30 минут в системе не производится никаких действий, осуществляется автоматический выход из системы. • **Автоматическая блокировка учётной записи** - после трёх неудачных попыток ввода пароля для входа в систему учётная запись автоматически блокируется. • **Протоколирование действий** - ведется протоколирование всех действий в системе	• **Защита от перехвата документов по каналу** осуществляется с помощью защищённого файлового обмена между системами клиента и файловым сервером Банка по протоколу SFTP (SSH File Transfer Protocol). • **Защита от подделки документов и их передача в неизменном виде** обеспечивается электронной подписью по стандарту ГОСТ Р 34.10-2012. • **Шифрование передаваемых данных** по алгоритму PGP с длиной ключа 1024 бита. • **Протоколирование действий** - ведется детальное протоколирование всех действий.

Кроме того, клиент имеет возможность дополнительно снизить вышеуказанные риски, используя следующие ограничения:

Ограничение	Применимость	
	Business.Online	Host-to-Host
Ограничить передачу электронных документов по IP/MAC-адресам	Да	Да
Ограничить права уполномоченных лиц на доступ к счетам и/или типам электронных документов	Да	Нет[1]

[1] Настраивается в системах клиента.

Установить для уполномоченных лиц порядок и/или сочетание категорий подписей, используемых для подписания и авторизации электронных документов	Да	Да
Установить для уполномоченных лиц лимиты сумм подписываемых распоряжений	Да	Нет[1]

Также, клиенту необходимо:

- обеспечить информационную безопасность (в том числе защиту от вредоносного кода/ вирусов/ «шпионского» программного обеспечения и т.д.) рабочих мест сотрудников, уполномоченных осуществлять электронный документооборот с Банком, а также исключить доступ к ним неуполномоченных лиц;
- при изменении перечня уполномоченных лиц, в том числе в связи с увольнением уполномоченного лица, необходимо незамедлительно представить в Банк заявку на изменение списка уполномоченных лиц в порядке, установленном в соответствующей договорной документации;
- обеспечить ознакомление уполномоченных лиц с «Памяткой по информационной безопасности пользователя электронного документооборота» (Приложение 1 к настоящим Условиям).

Памятка по информационной безопасности
пользователя электронного документооборота

1. Перед вводом логина и пароля для доступа в систему Business.Online убедитесь, что в адресной строке web-браузера отображается «https://gws.unicredit.ru». В противном случае прекратите ввод данных и незамедлительно сообщите о данном факте по телефону Банка +7(800)700-10-20, +7(495)725-25-44.

2. Используйте сложные пароли, состоящие не менее чем из 8 различных символов (обязательно использование цифр, латинских букв, специальных символов). Не сообщайте посторонним лицам Ваши логины и пароли, не записывайте их и не используйте функцию запоминания логина и пароля в браузерах. Не используйте одинаковые логин и пароль для доступа в различные системы электронного документооборота. Регулярно производите смену паролей.

3. Запрещается хранить пароли на носителе ключей электронной подписи, носителе одноразовых паролей и мобильном устройстве, используемом для получения одноразовых SMS-паролей, а также на иных электронных носителях, доступ к которым могут получить третьи лица, в том числе в случае заражения устройства вирусом.

Помните, что сотрудник Банка не имеет права запрашивать у Вас пароли. Банк никогда не отправляет сообщения с просьбой уточнить или предоставить пароль. При получении просьбы, в том числе от имени сотрудника Банка, сообщить персональные данные или информацию о паролях - не сообщайте их.

4. Обеспечьте предотвращение несанкционированного доступа к носителю ключей электронной подписи (USB-токену), не передавайте его третьим лицам и храните в месте, доступном только Вам. Отключайте носитель ключей электронной подписи от устройства доступа даже при кратковременном прекращении работы.

5. В случае подозрений в утере (краже) и/или в несанкционированном доступе третьих лиц к логину/паролю, носителю ключей электронной подписи, носителю одноразовых паролей и устройству мобильной связи, используемому для получения одноразовых SMS-паролей, незамедлительно прекратите использование системы Business.Online/технологии Host-to-Host и сообщите об этом в Банк по телефонам +7(800)700-10-20, +7(495)725-25-44.

6. После окончания работы завершите сеанс с помощью кнопки «Выход».

7. Исключите возможность доступа посторонних лиц к устройству доступа, в том числе в целях установки программного обеспечения.

8. Не используйте права администратора при отсутствии необходимости. В повседневной работе рекомендуется использовать учётную запись с минимально необходимым набором прав.

9. Применяйте актуальные средства антивирусной защиты на компьютерах, используемых для осуществления электронного документооборота. Установите регулярную автоматическую антивирусную проверку. Проверяйте все съёмные носители информации (USB-Flash, CD/DVD-диски, карты памяти SD и т.п.) до начала их использования.

10. При возникновении подозрений в нарушении информационной безопасности Вашего средства доступа (в том числе от вредоносного кода/ вируса/ «шпионского» программного обеспечения и т.д.), незамедлительно заблокируйте доступ к электронному документообороту, обратившись в Банк по телефону +7(800)700-10-20, +7(495)725-25-44.