Утверждено
Правлением АО «Альянс-Банк»
Протокол №47
От 15 сентября 2014г.

Правила предоставления электронных банковских услуг для юридических лиц/индивидуальных предпринимателей посредством систем «Интернет-банкинг для юридических лиц/ Интернет-банкинг для юридических лиц «ForteBusiness» и Мобильный интернет-банкинг «ForteBusiness» в АО «ForteBank»

КС- 02П-СУОД-027

В наименование документа внесены изменения согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021г.

РАЗРАБОТЧИК:
Направление развития продуктов МСБ и сервиса

г. Нур-Султан
2014 год

1. Общие положения

Настоящие Правила предоставления электронных банковских услуг для юридических лиц/индивидуальных предпринимателей посредством Систем «Интернет-банкинг для юридических лиц/ Интернет-банкинг для юридических лиц «ForteBusiness» и Мобильный интернет- банкинг «ForteBusiness»» в АО «ForteBank», (далее по тексту именуемые «Правила»), разработаны в соответствии с действующим законодательством Республики Казахстан, внутренними документами АО «ForteBank» и предусматривают порядок и условия предоставления электронных банковских услуг юридическим лицам/индивидуальным предпринимателям посредством Систем «Интернет-банкинг для юридических лиц/ Интернет-банкинг для юридических лиц «ForteBusiness» и Мобильный интернет- банкинг «ForteBusiness»».

При первичной идентификации (регистрации) в системах «Интернет-банкинг для юридических лиц/ Интернет-банкинг для юридических лиц «ForteBusiness» и Мобильный интернет-банкинг «ForteBusiness», Клиент (его представитель) предоставляет согласие на сбор и обработку его персональных данных в целях предоставления Клиенту электронных банковских услуг.

Пункт дополнен новым абзацем согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

(По всему тексту Правил внесены изменения согласно решению Правления №39 от 09.07.2015).
(По всему тексту Правил внесены изменения согласно решению Правления №49 от 25.06.2015).
(По всему тексту Правил внесены изменения согласно решению Правления от 05 июля 2017 года (протокол заседания №53).
(По всему тексту Правил внесены изменения согласно решению Операционного комитета от 16 мая 2019 года (протокол заседания №16).
(По всему тексту Правил внесены изменения согласно решению Правления № 01/2021-78 от 09.07.2021 года).

2. Термины и определения, используемые в Правилах

1) **Аутентификация** – подтверждение подлинности и правильности составления электронного документа Клиента и его волеизъявления, путем использования Процедуры безопасности, установленной Банком;
2) **Банк** – АО "ForteBank";
3) **Банковский счет Клиента** – Текущий и/или Сберегательный счет Клиента, открытый в Банке;

3-1) Биометрическая идентификация – процедура установления личности Клиента с целью однозначного подтверждения его прав на получение электронных банковских услуг на основе его физиологических и биологических особенностей;

Дополнен пунктом 3-1) согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

4) **Договор** – Договор об оказании электронных банковских услуг посредством Систем "Интернет-банкинг для юридических лиц/Интернет-банкинг для юридических лиц «ForteBusiness» и Мобильный интернет банкинг", заключенный между Банком и Клиентом, с изменениями и дополнениями, а также любые дополнительные условия оказания Электронных банковских услуг, публикуемые на веб-сайте Банка www.forte.kz или иным образом доступные для Клиента, и оговоренные в Договоре;
5) **Заявка** – Заявка на предоставление доступа к Системе "Интернет-банкинг для юридических лиц"/«ForteBusiness», оформленная в соответствии с формой, установленной в Приложении №1 к Договору об оказании электронных банковских услуг/ Приложение 4 к Заявлению Системы Интернет-банкинг для юридических лиц/«ForteBusiness». Заявка Клиента подписывается его первым руководителем и скрепляется печатью Клиента (при наличии) или подписывается уполномоченным им лицом (и скрепляется печатью при указании об этом в соответствующей Доверенности);

5-1) Заявление – Заявление о присоединении к Общим условиям проведения операций по банковским счетам клиентов с использованием системы (приложение № 4 к Положению о порядке предоставления отдельной категории клиентов ряда банковских услуг на условиях присоединения к Общим условиям банковского обслуживания);

6) **Идентификация Клиента** – процедура установления подлинности Пользователя/Уполномоченного лица Клиента с целью однозначного подтверждения его прав на получение Электронных банковских услуг;
7) **Клиент** – юридическое лицо/индивидуальный предприниматель, заключившие Договор;
8) **Контактные данные** – контактные телефоны и адреса Банка/ответственных работников Банка для обращения Клиентов по вопросам, связанным с предоставлением Электронных банковских услуг;
9) **Логин клиента** – уникальный логин Клиента (используемый совместно с Логином пользователя), предоставляется Банком один для всех Пользователей/Уполномоченных лиц Клиента, в целях

регистрации в Системе и последующего доступа к Электронным банковским услугам через Систему «Интернет-банкинг для юридических лиц»;

10) Логин пользователя – уникальный логин Пользователя/Уполномоченного лица Клиента в Системе, предоставляемый Банком в целях регистрации в Системе и последующего доступа к Электронным банковским услугам через Систему;

10-1) Мобильный интернет-банкинг «ForteBusiness» (Мобильный интернет- банкинг) -программное обеспечение, предназначенное для осуществления банковских операций Клиентом – индивидуальным предпринимателем[1] в личном кабинете посредством мобильного телефона или иного устройства, поддерживающего мобильное приложение и доступ в интернет;

Дополнен пунктом 10-1) согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

10-2) НУЦ РК – Национальный удостоверяющий центр Республики Казахстан, предоставляющий средства электронной цифровой подписи и регистрационные свидетельства физическим или юридическим лицам для формирования электронных документов в государственных и негосударственных информационных системах;

Дополнен пунктом 10-2) согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

11) ПИН для входа в систему – персональный идентификационный номер, необходимый для входа в Систему. Предоставляется Банком каждому Пользователю/Уполномоченному лицу Клиента в открытом виде, смена которого требуется при первом входе в Систему «Интернет-банкинг для юридических лиц», состоящий из букв, символов и специальных символов;

11-1) Пароль – совокупность цифровых, буквенных и иных символов, предназначенная для подтверждения прав Клиента на вход в Систему Банка для получения Электронных банковских услуг;

11-2) Общие условия – Общие условия дистанционного обслуживания с использованием систем «Интернет-банкинг для юридических лиц/ Интернет-банкинг для юридических лиц «ForteBusiness» и мобильный интернет-банкинг «ForteBusiness»;

12) ПИН – персональный идентификационный номер, необходимый для активации Устройства Digipass в целях получения Сгенерированного кода. Предоставляется Банком каждому Пользователю/Уполномоченному лицу Клиента;

12-1) ПИН-код для быстрого входа- секретный набор чисел, с помощью которого Клиент может получить доступ в Мобильный интернет- банкинг;

Дополнен пунктом 12-1) согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

13) Подключение Клиента к Системе – регистрация Пользователей/Уполномоченных лиц Клиента в Системе, согласно условиям Договора и Заявке Клиента;

14) Подразделение Филиала – дополнительное помещение Филиала Банка - Управление Бизнес продаж или Центр банковского обслуживания, расположенные по нескольким адресам в пределах одной области (города республиканского значения, столицы);

15) Процедуры безопасности – комплекс организационных мер и программно-технических средств защиты информации, предназначенных для идентификации Пользователя/Уполномоченного лица Клиента при подключении к Системе, составлении, передаче и получении электронных документов с целью установления его права на получение Электронных банковских услуг и обнаружения ошибок и/или изменений в содержании передаваемых и получаемых электронных документов;

16) Пользователь Клиента (Пользователь) – уполномоченное в установленном законодательством Республики Казахстан порядке лицо, указанное Клиентом в Заявке, которому, в соответствии с Договором, предоставляется право доступа к Системе и возможность осуществления необходимых действий для получения Клиентом Электронных банковских услуг, за исключением прав подписания и направления электронных документов Банку от имени Клиента;

17) Представитель Клиента – лицо, уполномоченное Клиентом соответствующей Доверенностью получать от Банка все необходимые сведения, устройства и документы для надлежащего использования Системы Клиентом, а также выполнять иные действия в целях получения услуг в рамках Договора;

18) Рабочие дни – дни, не являющиеся выходными либо праздничными, в соответствии с законодательством Республики Казахстан;

19) Сгенерированный код – одноразовый (единовременный) код, уникальная последовательность электронных цифровых символов, создаваемая программно-аппаратным средством Банка (Устройство

---

[1] *До осуществления технической реализации процесса обслуживания юридических лиц в мобильном интернет-банкинге указанный в настоящих Правилах порядок Идентификации, Аутентификации и в целом использование мобильного интернет-банкинга распространяется исключительно в отношении Клиентов – индивидуальных предпринимателей.*

Digipass), и предназначенная для разового использования при предоставлении доступа Клиенту к Электронным банковским услугам;

20) **Система** – Система – программное обеспечение «Интернет-банкинг для юридических лиц/ Интернет-банкинг для юридических лиц «ForteBusiness»/ Мобильный интернет- банкинг «ForteBusiness», посредством которого Банк предоставляет Клиенту электронные банковские услуги. Доступ к Системе осуществляется через Интернет посредством веб-адреса Системы «Интернет-банкинг для юридических лиц» (https://online.fortebank.com) / Интернет-банкинг для юридических лиц «ForteBusiness» (https://ibank.forte.kz/), а также посредством мобильного телефона или иного устройства, поддерживающего мобильное приложение и доступ в интернет (IOS, Android);

Пункт дополнен понятием мобильный интернет-банкинг согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

21) **Сберегательный счет** – банковский счет, открываемый Банком Клиенту на основании договора банковского вклада для выполнения операций, предусмотренных Договором банковского вклада, в соответствии с требованиями действующего законодательства Республики Казахстан";

22) **Текущий счет** – банковский счет, открываемый Банком Клиенту на основании договора банковского счета, по которому выполняются операции, предусмотренные договором банковского счета, в соответствии с требованиями законодательства Республики Казахстан;

23) **ForteX** - модуль/раздел программного обеспечения "Интернет-банкинг и мобильный интернет банкинг для юридических лиц"/ «ForteBusiness» для предоставления Банком электронных банковских услуг посредством электронных заявок;

24) **Устройство Digipass** – электронное устройство (программно-аппаратное средство), генерирующее/создающее Сгенерированный код, предоставленное Банком Клиенту в соответствии с условиями Договора и настоящими Правилами. Для активации Устройства Digipass используется ПИН. Правила эксплуатации Устройства Digipass предусмотрены в Приложении №1 к настоящим Правилам;

25) **Уполномоченный орган –** государственные органы Республики Казахстан или иные должностные лица, уполномоченные налагать арест на деньги на банковских счетах и/или приостанавливать расходные операции по банковским счетам, согласно законодательству Республики Казахстан;

26) **Уполномоченное лицо Клиента** – Пользователь/Лицо Клиента, указанное в документе с образцами подписей и оттиска печати Клиента, предоставляемом Клиентом Банку в соответствии с законодательством Республики Казахстан при открытии Банковского счета Клиента/проведении операций в модуле ForteX, которое вправе подписывать и направлять электронные документы Банку от имени Клиента;

27) **Филиал** – обособленное подразделение Банка, осуществляющее банковские операции, в которое обращается Клиент;

28) **Электронные банковские услуги (Услуги)** – банковские услуги, предоставляемые Банком Клиенту дистанционно через Систему в порядке и на условиях, установленных нормативными правовыми актами Республики Казахстан, Договором и настоящими Правилами;

28-1) **Электронный документ –** документ, в котором информация представлена в электронно-цифровой форме и удостоверена идентификационными средствами, составленный отправителем и не содержащий искажений и (или) изменений, внесенных в него после составления, в порядке, предусмотренном законодательством Республики Казахстан;

29) **Электронная заявка -** заявка, направляемая Клиентом для проведения конвертации в модуле ForteX, посредством Системы "Интернет-банкинг для юридических лиц"/ «ForteBusiness». Электронная заявка Клиента подписывается Уполномоченным лицом Клиента";

29-1) **СМС – код** – одноразовый (единовременный) код, состоящий из уникальных последовательных электронных цифровых символов, создаваемый программно-техническими средствами Банка по запросу пользователя направленный посредством sms-сообщения на номер мобильного телефона Уполномоченного лица клиента, указанный в Заявке и предназначенный для одноразового использования при предоставлении доступа пользователю к электронным банковским услугам, используемый в системе «ForteBusiness»;

29-2) **Электронно-цифровая подпись (ЭЦП) -** набор электронных цифровых символов, созданный средствами ЭЦП и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания, являющийся идентификационным средством;

Дополнен пунктом 29-2) согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

29-3) **FaceID-** сканер объёмно-пространственной формы лица Клиента, с помощью которого можно безопасно разблокировать устройство, выполнять вход в Мобильный интернет -банкинг;

Дополнен пунктом 29-3) согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

29-4) TouchID- система идентификации Клиента по отпечатку пальца, с помощью которого можно безопасно разблокировать устройство, выполнять вход в Мобильный интернет-банкинг;

Дополнен пунктом 29-4) согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

29-5) **SMS-верификация-** процесс динамической идентификации посредством направления Клиенту SMS-сообщения на номер мобильного телефона, содержащего СМС – код, который вводится при Идентификации или Аутентификации в Мобильном интернет-банкинге с целью однозначного подтверждения его прав на получение электронных банковских услуг.

Дополнен пунктом 29-5) согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

(Раздел 2 Правил изложен в новой редакции согласно решению Правления от 05 июля 2017 года (протокол заседания №53).

(В раздел 2 Правил внесены дополнения согласно решению Правления № 01/2021-78 от 09.07.2021 года).

3. Перечень электронных банковских услуг

Банк оказывает Клиенту Электронные банковские услуги в порядке и на условиях, установленных Договором и настоящими Правилами.

1. Электронные банковские услуги включают:

1.1. Информационно-банковские услуги:

1.1.1. предоставление доступа к банковским счетам клиентов, подключенным к Системе согласно Заявке;

1.1.2. предоставление информации об остатках и (или) движении денег по Банковским счетам Клиента, о платежах и(или) переводах денег, осуществленных по счетам Клиента;

1.1.3. настройка списков получателей платежей (бенефициаров), включая внесение необходимых изменений;

1.1.4. просмотр истории платежей и (или) переводов;

1.1.5. создание шаблонов для осуществления однотипных платежей и (или) переводов в будущем;

1.1.6. связь с Банком через канал безопасных соединений посредством электронных сообщений (срок и порядок предоставления ответа Банка определяется Правилами об общих условиях проведения банковских операций АО «ForteBank»);

1.1.7. открытие банковского счета[2].

Дополнен пунктом 1.1.7 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

1.2. Платежные услуги:

1.2.1. осуществление платежей и (или) переводов денег в тенге и в иностранной валюте, находящихся на Банковских счетах Клиента;

1.2.2. осуществление покупки и продажи иностранной валюты, проведение конверсионных операций;

1.2.3. создание, изменение, либо отмена постоянно действующих инструкций (электронных документов) по Банковским счетам Клиента;

1.2.4. создание электронных документов по осуществлению платежей и переводов по Банковским счетам Клиента на будущую дату;

1.2.5. выпуск/обслуживание платежных карточек[3].

Дополнен пунктом 1.2.5 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

1.3. Иные услуги:

1.3.1. подача заявлений для получения банковских услуг посредством системы "ForteBusiness".

2. Данный перечень не является исчерпывающим и может быть дополнен/изменен Банком в одностороннем порядке по мере развития систем, о чем Банк извещает своих Клиентов посредством размещения соответствующего информационного сообщения на официальном сайте Банка www.forte.kz.

(В раздел 3 Правил внесены изменения согласно решению Правления от 05 июля 2017 года (протокол заседания №53).

(В раздел 3 Правил внесены дополнения согласно решению Операционного комитета от 16 мая 2019 года (протокол заседания №16).

(В раздел 3 Правил внесены дополнения согласно решению Правления № 01/2021-78 от 09.07.2021 года).

---

[2] *доступно только в мобильном интернет-банкинге*

[3] *доступно только в мобильном интернет-банкинге*

4. Порядок, способ и условия предоставления электронных банковских услуг

3. Доступ Клиента к Электронным банковским услугам предоставляется удаленно по защищенным каналам связи через Интернет с любого устройства, имеющего доступ к сети Интернет.

4. Доступ Клиента к Электронным банковским услугам возможен только после и при условии заключения Договора и прохождения регистрации одного из Пользователей/Уполномоченных лиц Клиента в Системе, указанных в Заявке Клиента.

5. Предоставление Информационно-банковских услуг осуществляется при условии Идентификации и успешной Аутентификации Клиента.

6. Предоставление платежных услуг осуществляется при условии Идентификации Клиента и успешной Аутентификации в соответствии с Процедурами безопасности. При этом предоставление платежных услуг осуществляется только при условии регистрации Уполномоченных лиц Клиента, обладающих необходимыми и достаточными правами предоставления электронных документов Клиента Банку для получения платежных услуг. При Аутентификации используется динамическая идентификация Клиента при помощи Устройства Digipass.

(В раздел 4 Правил внесены дополнения согласно решению Операционного комитета от 16 мая 2019 года (протокол заседания №16).

7. Порядок и условия регистрации Пользователя/Уполномоченного лица Клиента в Системе «Интернет-банкинг для юридических лиц».

7.1. Регистрация Пользователя/Уполномоченного лица Клиента в Системе «Интернет-банкинг для юридических лиц» осуществляется через Интернет с любого компьютера, имеющего доступ к сети Интернет. При этом Пользователь/Уполномоченное лицо обязан/о соблюдать Процедуры безопасности.

7.2. Для регистрации Пользователя/Уполномоченного лица Клиента в Системе «Интернет-банкинг для юридических лиц» Пользователю/Уполномоченному лицу Клиента необходимо получить в Банке Логин Клиента, Логин пользователя, ПИН для входа в систему (первичный), ПИН (первичный), Устройство Digipass.

7.3. Логин Клиента, Логин Пользователя формируются Банком самостоятельно без участия Клиента.

7.4. Логин Клиента, Логин пользователя, ПИН для входа в систему (первичный), ПИН (первичный), Устройство Digipass предоставляются Пользователю/Уполномоченному лицу Клиента в течение 10 (десяти) Рабочих дней, с даты заключения Договора при личной явке Пользователя/Представителя Клиента в Банк и при условии подписания Пользователем/Представителем Клиента Акта приема-передачи по форме, установленной Договором.

7.5. Регистрация Пользователя/Уполномоченного лица Клиента в Системе «Интернет-банкинг для юридических лиц» осуществляется через соответствующий веб-адрес Системы «Интернет-банкинг для юридических лиц», путем внесения Пользователем/Уполномоченным лицом Клиента Логина Клиента, Логина пользователя, ПИН для входа в систему и Сгенерированного кода.

7.6. В целях соблюдения Процедур безопасности, при получении Устройства Digipass, Пользователь/Уполномоченное лицо обязан/о сменить первичный ПИН, полученный от Банка на персональный ПИН согласно требованиям Процедур безопасности, условиям настоящих Правил и Приложения №1 к Правилам.

7.7. ПИН для входа в систему (первичный) выдается Пользователю/Уполномоченному лицу Клиента в открытом виде, в целях соблюдения Процедур безопасности, при первом входе в Систему «Интернет-банкинг для юридических лиц», требуется его смена на персональный ПИН для входа в систему.

7.8. В случае утери/утраты Логина пользователя и/или ПИН для входа в систему и/или ПИН и/или Устройства Digipass и/или поломки Устройства Digipass, Пользователь/Уполномоченное лицо Клиента вправе получить новые Логин пользователя и/или ПИН для входа в систему (первичный) и/или ПИН (первичный) и/или Устройство Digipass на основании надлежащим образом оформленного письма Клиента. Получение нового(ых) Логина пользователя и/или ПИН для входа в систему (первичный) и/или ПИН (первичный) и/или Устройство Digipass осуществляется при личной явке Клиента/Пользователя/Представителя Клиента в Банк и при условии подписания Клиентом/Пользователем/Представителем Клиента Акта приема-передачи по форме, установленной Договором.

7.9. Подключение Банковских счетов Клиента к Системе «Интернет-банкинг для юридических лиц» для получения Электронных банковских услуг и исключение их из Системы «Интернет-банкинг для юридических лиц» осуществляется в соответствии с условиями Договора.

7.10. Подключение Клиента к Системе «Интернет-банкинг для юридических лиц» осуществляется в соответствии с условиями Договора.

7-1. Порядок и условия регистрации Пользователя /Уполномоченного лица Клиента в Системе «ForteBusiness»:

7-1.1. Регистрация Пользователя/ Уполномоченного лица Клиента в Системе осуществляется через Интернет с любого устройства, имеющего доступ к сети Интернет. При этом Пользователь/Уполномоченное лицо обязан/о соблюдать Процедуры безопасности.

7-1.2. Для регистрации Пользователя/Уполномоченного лица Клиента в Системе Пользователю/Уполномоченному лицу Клиента необходимо получить в Банке Логин пользователя, Пароль, ПИН (первичный), Устройство Digipass.

7-1.3. Логин Пользователя, Пароль, ПИН, Устройство Digipass предоставляются Пользователю/Уполномоченному лицу Клиента в течение 10 (десяти) Рабочих дней, с даты подписания заявки на предоставление доступа к системе, при личной явке Пользователя/Представителя Клиента в Банк и при условии подписания Пользователем/Представителем Клиента Акта приема-передачи по форме.

7-1.4. Регистрация Пользователя /Уполномоченного лица Клиента в Системе осуществляется через соответствующий адрес веб-адрес Системы, путем внесения Пользователем/Уполномоченным лицом Клиента Логина пользователя, Пароля и Сгенерированного кода.

7-1.5. В целях соблюдения Процедур безопасности, при получении Устройства Digipass, Пользователь/Уполномоченное лицо обязан/о сменить первичный ПИН, полученный от Банка на персональный ПИН согласно требованиям Процедур безопасности, условиям настоящих Правил и Приложения №1 к Правилам.

7-1.6. Первичный Пароль выдается Пользователю/Уполномоченному лицу Клиента в открытом виде, в целях соблюдения Процедур безопасности, при первом входе в Систему, требуется его смена на персональный Пароль.

7-1.7. В случае ПИН и/или Устройства Digipass и/или поломки Устройства Digipass, Пользователь/Уполномоченное лицо Клиента вправе получить ПИН и/или Устройство Digipass на основании надлежащим образом оформленного письма Клиента. Получение нового(ых) ПИН и/или Устройство Digipass осуществляется при личной явке Клиента/Пользователя/Представителя Клиента в Банк и при условии подписания Клиентом/Пользователем/Представителем Клиента Акта приема-передачи по форме.

В случае неверного ввода Пароля 3 (три) раза подряд, Система «ForteBusiness» блокирует возможность входа в Систему. Доступ в Систему «ForteBusiness» Клиенту может быть предоставлен после сброса и/или восстановления Пароля. Для смены Пароля необходимо нажатие Клиентом на значок «Восстановление пароля» в основном окне, после чего Банком будет выслан СМС-код на номер сотового телефона Клиента. Если Клиент забыл Пароль для доступа в Систему «ForteBusiness», он вправе применить указанные выше действия. Восстановление пароля Банком может быть осуществлено через генерацию одноразового Пароля по обращению Клиента/Пользователя/Представителя Клиента.

7-1.8. Подключение Банковских счетов Клиента к Системе для получения Электронных банковских услуг и исключение их из Системы осуществляется в соответствии с условиями заявки на подключение.

7-1.9. Подключение Клиента к Системе осуществляется в соответствии с условиями заявления о присоединении к Общим условиям проведения операций по банковским счетам клиентов с использованием системы.

7-2. Порядок и условия Идентификации (регистрации) Клиента в Мобильном интернет-банкинге:

Дополнен пунктом 7-2 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

7-2.1 Первичная Идентификация (регистрация) Клиента в Мобильном интернет-банкинге осуществляется посредством мобильного телефона или иного устройства, поддерживающего мобильное приложение Банка и доступ в Интернет. При этом Клиент обязан соблюдать Процедуры безопасности.

Дополнен пунктом 7-2.1 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

7-2.2 Первичная Идентификация (регистрация) Клиента в Мобильном интернет-банкинге осуществляется одним из двух способов:

1. Путем проведения SMS-верификации и биометрической идентификации (Клиентом вводится также индивидуальный идентификационный номер);
2. С использованием ЭЦП и SMS-верификации (индивидуальный идентификационный номер вводится автоматически на основании данных, полученных из ЭЦП).

При первичной Идентификации (регистрации) в Мобильном интернет-банкинге Клиенту необходимо установить Пароль, логином будет выступать номер его мобильного телефона. Кроме того, Клиенту предлагается установить FaceID, TouchID и ПИН-код для быстрого входа.

Дополнен пунктом 7-2.2 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

7-2.3 Последующий вход в Мобильный интернет-банкинг осуществляется путем введения Клиентом логина и Пароля, а также с использованием SMS-верификации, либо использования FaceID/TouchID/ПИН-кода быстрого входа. При установлении FaceID/TouchID/ПИН-кода быстрого входа Мобильный интернет-банкинг запоминает введенные Клиентом логин и Пароль и при каждом использовании FaceID/TouchID/ПИН-кода быстрого входа автоматически вводится Пароль для входа в Мобильный интернет-банкинг. При присоединении к Общим условиям Клиент соглашается с указанным способом входа в Мобильный интернет-банкинг.

Дополнен пунктом 7-2.3 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

7-2.4 Клиенту необходимо не разглашать/не передавать третьим лицам и обеспечить сохранность Пароля и ПИН-кода быстрого входа, а также не устанавливать на мобильное/иное устройство FaceID/TouchID третьих лиц в целях исключения несанкционированного доступа в Мобильный интернет- банкинг.

Дополнен пунктом 7-2.4 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

7-2.5 Изменение номера мобильного телефона, используемого для входа Клиентом в Мобильный интернет-банкинг осуществляется Клиентом самостоятельно в Мобильном интернет-банкинге путём подписания Приложения №2 к Общим условиям.

Дополнен пунктом 7-2.5 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

7-2.6 В случае неверного ввода Пароля 3 (три) раза подряд, Система блокирует возможность входа в Мобильный интернет-банкинг. Доступ в Систему Клиенту может быть предоставлен после сброса и восстановления Пароля. Для смены Пароля необходимо нажатие Клиентом на значок на стартовой странице.

Дополнен пунктом 7-2.6 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

7-2.7 Предоставление электронных банковских услуг в Системе осуществляется на основании присоединения к Общим условиям путем подачи Заявления.

Дополнен пунктом 7-2.7 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

(В раздел 4 Правил внесены дополнения согласно решению Операционного комитета от 16 мая 2019 года (протокол заседания №16).

(В раздел 4 Правил внесены дополнения согласно решению Правления № 01/2021-78 от 09.07.2021 года).

8. Порядок и условия предоставления Информационно-банковских услуг:

8.1. Пункт 8.1. исключен согласно решению Правления от 05 июля 2017 года (протокол заседания №53).

8.2. Порядок Идентификация и Аутентификация Пользователя/Уполномоченного лица Клиента в Системе «Интернет-банкинг для юридических лиц».

8.2.1. Идентификация и Аутентификация Клиента в Системе производятся путем введения Пользователем/Уполномоченным лицом Клиента в соответствующем электронном окне Системы надлежащего Логина Клиента, Логина пользователя, ПИН для входа в систему и Сгенерированного кода.

8.2.2. В случае правильного указания Пользователем//Уполномоченным лицом Клиента Логина Клиента, Логина пользователя, ПИН для входа в систему и Сгенерированного кода, Идентификация Клиента в Системе признается осуществленной надлежащим образом, и Пользователь/Уполномоченное лицо Клиента получает доступ к Электронным банковским услугам.

8.3. Порядок Идентификация и Аутентификация Пользователя/Уполномоченного лица Клиента в Системе «ForteBusiness».

8.3.1. Идентификация Клиента в Системе производятся путем введения Пользователем/Уполномоченным лицом Клиента в Системе «ForteBusiness» в соответствующем электронном окне Системы надлежащего Логина, Пароля и Сгенерированного кода.

8.3.2. Аутентификация производится путем подписания Пользователем/Уполномоченным лицом Клиента Электронных документов с использованием Сгенерированного кода.

8.4. После получения доступа Пользователь/Уполномоченное лицо Клиента вправе самостоятельно получать Информационно-банковские услуги, посредством Системы.

8.5. Порядок Аутентификации Клиента в Мобильном интернет- банкинге:

Дополнен пунктом 8.5 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

8.5.1. Аутентификация производится путем подписания Клиентом Электронных документов с использованием SMS-верификации или ЭЦП.

Дополнен пунктом 8.5.1. согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

8.5.2. После получения доступа в Мобильный интернет-банкинг Клиент вправе самостоятельно получать Информационно-банковские услуги.

Дополнен пунктом 8.5.2. согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

8.5.3. Интерфейс Мобильного интернет-банкинга функционирует на русском и казахском языках по выбору Клиента.

Дополнен пунктом 8.5.3. согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

(В раздел 4 Правил внесены дополнения согласно решению Операционного комитета от 16 мая 2019 года (протокол заседания №16).

(В раздел 4 Правил внесены дополнения согласно решению Правления № 01/2021-78 от 09.07.2021 года).

9. Порядок и условия предоставления платежных услуг:

9.1. Пункт 9.1. исключен согласно решению Правления от 05 июля 2017 года (протокол заседания №53).

9.2. В целях установления подлинности Клиента производится Идентификация Клиента путем введения Пользователем/Уполномоченным лицом ПИН для входа в систему/ Пароля и Сгенерированного кода, созданного Устройством Digipass. Идентификация производится с целью однозначного подтверждения его прав на получение электронных банковских услуг.

9.3. В случае надлежащей Аутентификации, Клиенту предоставляются платежные услуги.

9.4. Платежные услуги предоставляются на основании электронных документов Клиента при условии их акцепта Банком.

9.5. При получении платежных услуг, Клиент использует формы электронных документов, формирующихся в Системе автоматически и соответствующих действующему законодательству Республики Казахстан.

9.6. Электронные документы оформляются Пользователем и подписываются Уполномоченным лицом Клиента. В случаях, когда платежные документы Клиента должны быть подписаны несколькими Уполномоченными лицами Клиента, обладающими правом подписи, электронные документы Клиента считаются надлежащим образом предоставленными Банку только после подписания электронных документов Уполномоченными лицами в соответствии с поручениями Клиента и требованиям законодательства Республики Казахстан.

9.7. Платежи и (или) переводы в иностранной валюте, через Систему осуществляются с соблюдением законодательства Республики Казахстан о валютном регулировании и валютном контроле.

9.7.1. Курс обмена валют, применяемого при оказании электронных банковских услуг в иностранной валюте определяется Банком на момент проведения операции.

9.8. Пункт 9.8. исключен согласно решению Правления от 05 июля 2017 года (протокол заседания №53).

9.9. Банк может отказать в акцепте электронных документов в случаях, предусмотренных действующим законодательством Республики Казахстан, а также в иных случаях, предусмотренных Договором и соответствующими договорами банковского счета.

(В пункт 9 Главы 4 внесены изменения согласно решению Правления от 05 июля 2017 года (протокол заседания №53).

4-1.Проведение конвертации в модуле ForteX

9.9-1. Проведение конвертации посредством модуля ForteX осуществляется с соблюдением законодательства Республики Казахстан о валютном регулировании и валютном контроле.

9.9-2 Курс обмена валют, применяемого при проведении конвертации в ForteX определяется Банком и действует в течении ограниченного времени с момента подтверждения Клиентом курса.

9.9-3.Акцепт и подписание электронной Заявки на конвертацию в модуле ForteX в течение ограниченного времени производится всеми Уполномоченными лицами Клиента на подписание заявки в модуле ForteX.

9.9-4.Исполнение Банком электронной Заявки на конвертацию в модуле ForteX осуществляется в автоматическом режиме. В случае ввода некорректных данных при оформлении электронной заявки, указанная электронная заявка не подлежит отмене.

9.9-5. Допускается проведение конвертации в модуле ForteX Уполномоченным лицом Клиента, указанным в отдельном документе с образцами подписей и оттиском печати (при наличии), который предоставляется в Банк до проведения операции в модуле ForteX вместе с соответствующей доверенностью на такое уполномоченное лицо Клиента (при необходимости);

9.9-6. При проведении операций в модуле ForteX, клиент:

1) признает, что получение Банком документов посредством модуля ForteX юридически эквивалентно получению документов на бумажном носителе, оформленных в соответствии с требованиями законодательства РК и подписанных клиентом собственноручно;

2) несет полную ответственность за содержание документов, отправленных Банку посредством модуля ForteX для исполнения и за правовые последствия, порождаемые такими документами;

3) берет на себя ответственность и обязательство за санкционированность документов, отправленных от имени Клиента посредством модуля ForteX и принятых Банком к исполнению в соответствии с установленными процедурами безопасности.

(Правила дополнены Разделом 4-1 согласно решению Правления от 05 июля 2017 года (протокол заседания №53).

5. Приостановление/возобновление и прекращение предоставления электронных банковских услуг

10. Порядок и условия приостановления предоставления Электронных банковских услуг.

10.1. Банк вправе без предварительного уведомления Клиента приостановить предоставление Электронных банковских услуг и/или приостановить доступ Пользователя/Уполномоченного лица Клиента к Электронным банковским услугам в следующих случаях:

10.1.1. утери/разглашения/передачи третьим лицам Уполномоченным лицом/Пользователем Клиента Логина Клиента и/или Логина пользователя и/или ПИН для входа в систему и/или ПИН и/или Сгенерированного кода и/или Устройства Digipass, при получении Банком от Клиента соответствующего устного или письменного обращения;

10.1.2. при возникновении подозрений на угрозу несанкционированного доступа к Банковским счетам Клиента или несанкционированного использования Систем;

10.1.3. при наложении ареста и/или приостановлении расходных операций и/или наличии неисполненных требований третьих лиц на Банковском счете Клиента, по которому предоставляется Электронная банковская услуга.

10.1.4. в иных случаях, предусмотренных Договором и/или законодательством Республики Казахстан.

10.2. В случае утери/разглашения/передачи третьим лицам Пользователем/Уполномоченным лицом Клиента Логина Клиента и/или Логина пользователя и/или ПИН для входа в систему и/или ПИН и/или Сгенерированного кода и/или Устройства Digipass, приостановление предоставления Электронных банковских услуг и/или приостановление доступа Пользователя/Уполномоченного лица Клиента к Электронным банковским услугам может быть произведено Банком на основании устного обращения Пользователя/Уполномоченного лица Клиента с указанием кодового слова в Банк по Контактным данным, если это установлено Договором.

10.3. При поломке устройства Digipass по вине Клиента при видимых внешних повреждениях устройства Digipass (треснут экран устройства и/или нанесено механическое повреждение) и/или блокировке устройства Digipass более 3-х раз вследствие неправильного введения ПИН более 5 раз подряд Клиентом/Уполномоченным лицом Клиента (Устройство Digipass выдает сообщение «LOCK DISABLED»), Банк на основании письменного обращения Клиента/Представителя Клиента осуществляет в течение не более 3 (трех) рабочих дней с даты поступления письменного обращения Клиента в Банк замену устройства Digipass на платной основе в соответствии с тарифами Банка. При этом нерабочее Устройство Digipass передается Клиентом/Представителем Клиента ответственному работнику Подразделения Филиала по Акту приема-передачи нерабочего Устройства Digipass с указанием причины нерабочего состояния Устройства Digipass, описанием обнаруженных повреждений Устройства Digipass / сообщения «LOCK DISABLED», подписанному в 2-х экземплярах ответственным работником Подразделения Филиала и Клиентом/Представителем Клиента.

10.4. В случае неработоспособности устройства Digipass, выявленной/установленной в период не более 3-х (трех) месяцев с момента выдачи устройства Digipass Клиенту/его уполномоченному лицу, при отсутствии видимых внешних повреждений/сообщения «LOCK DISABLED», Банк на основании письменного обращения Клиента/Представителя Клиента осуществляет замену устройства Digipass в порядке, предусмотренном пунктом 10.3 настоящих Правил, без взимания оплаты согласно тарифам Банка.

При установлении/выявлении неработоспособности устройства Digipass по любым основаниям после установленного в первом абзаце настоящего пункта срока, замена устройства Digipass осуществляется на платной основе в соответствии с тарифами Банка в порядке, предусмотренном пунктом 10.3 настоящих Правил.

10.5. В случае наложения ареста и/или приостановления расходных операций Уполномоченным органом и/или наличия неисполненных требований третьих лиц по банковскому счету клиента, по которому предоставляется Электронная банковская услуга, Банк приостанавливает предоставление Электронных банковских услуг до момента снятия ареста и/или возобновления расходных операций и/или исполнения всех неисполненных требований третьих лиц на Банковском счете Клиента, по которому предоставляется Электронная банковская услуга.

10.6. При приостановлении предоставления Электронных банковских услуг Клиенту на основании соответствующего надлежащим образом оформленного письма Клиента и/или если Клиент имеет задолженность перед Банком по оплате услуг за проведение банковских операций более чем 30 (тридцать) календарных дней, доступ к Электронным банковским услугам приостанавливается для всех Пользователей/Уполномоченных лиц Клиента. Приостановление доступа к Электронным банковским услугам для конкретного Пользователя/Уполномоченного лица Клиента не приостанавливает доступ к Электронным банковским услугам для иных Пользователей/Уполномоченных лиц Клиента.

(В раздел 5 Правил внесены дополнения согласно решению Операционного комитета от 16 мая 2019 года (протокол заседания №16).

(В раздел 5 Правил внесены дополнения согласно решению Правления № 01/2021-78 от 09.07.2021 года).

11. Порядок и условия возобновления предоставления Электронных банковских услуг.

11.1. Возобновление предоставления Электронных банковских услуг в случае утери/разглашения/передачи третьим лицам Клиентом Логина пользователя и/или ПИН для входа в систему/ Пароля и/или ПИН и/или Устройства Digipass производится на основании надлежащим образом оформленного письма Клиента и/или Заявки (Приложение №1 к Договору) после предоставления Клиенту нового(ых) Логина пользователя и/или ПИН для входа в систему (первичного) для Системы «Интернет-банкинг для юридических лиц»/ восстановления Пароля самостоятельно Пользователем/Уполномоченным лицом Клиента для Системы «ForteBusiness» и/или ПИН (первичного) и/или Устройства Digipass взамен утраченных соответственно. При этом ответственный работник Подразделения Филиала, в котором обслуживается Клиент, в течение не более 3 (трех) рабочих дней с даты письменного обращения Клиента в Банк готовит и передает Клиенту/Уполномоченному лицу Клиента новый(ые) Логин пользователя и/или ПИН для входа в систему (первичный) и/или ПИН (первичный) и/или Устройство Digipass, по Акту приема-передачи, подписанному Клиентом/Уполномоченным лицом Клиента и ответственным работником Подразделения Филиала.

11.2. Возобновление предоставления Электронных банковских услуг в случае блокировки Устройства Digipass после неверного указания Клиентом ПИН для включения Устройства Digipass более 5 (пяти) раз подряд производится на основании надлежащим образом оформленного письма Клиента. При этом снятие блокировки самостоятельно Банком по вышеуказанному основанию возможно не более 3 (трех) раз, в противном случае Устройство Digipass блокируется и подлежит замене в порядке, предусмотренном пунктом 10.3 настоящих Правил.

11.3. Возобновление предоставления Электронных банковских услуг, приостановленных по причине возникновения подозрений на угрозу несанкционированного доступа к Банковским счетам Клиента, производится на основании надлежащим образом оформленного письма Клиента и/или Заявки (Приложение №1 к Договору), и после смены Банком Пользователю/Уполномоченному лицу Клиента Логина пользователя, ПИН для входа в Систему «Интернет-банкинг для юридических лиц»/ восстановления Пароля самостоятельно Пользователем/Уполномоченным лицом Клиента в Системе «ForteBusiness» . При этом ответственный работник Подразделения Филиала, в котором обслуживается Клиент, в течение не более 3 (трех) рабочих дней с даты письменного обращения Клиента в Банк готовит и передает Клиенту/Уполномоченному лицу Клиента новый(ые) Логин пользователя и/или ПИН для входа в систему по Акту приема-передачи, подписанному Клиентом/Уполномоченным лицом Клиента и ответственным работником Подразделения Филиала, в соответствии Приложением №2 к Договору.

11.4. Возобновление предоставления Электронных банковских услуг при наложении ареста Уполномоченными органами и/или приостановлении расходных операций и/или наличии неисполненных требований третьих лиц на банковском счете клиента, по которому предоставляется Электронная банковская услуга, производится только после снятия ареста и/или возобновления расходных операций и/или исполнения всех неисполненных требований третьих лиц на Банковском счете Клиента, по которому предоставляется Электронная банковская услуга.

(В раздел 5 Правил внесены дополнения согласно решению Правления № 01/2021-78 от 09.07.2021 года).

12. Порядок и условия прекращения предоставления Электронных банковских услуг.

12.1. Банк вправе без предварительного уведомления Клиента прекратить предоставление Электронных банковских услуг в следующих случаях:

12.1.1. если Клиент имеет задолженность перед Банком по оплате услуг за проведение банковских операций более чем 30 (тридцать) календарных дней;

12.1.2. если все Банковские счета Клиента в Банке закрыты.

12.1.3. в иных случаях, предусмотренных Договором и/или законодательством Республики Казахстан.

12.2. Банк вправе прекратить предоставление Электронных банковских услуг в случае прекращения действия/расторжения Договора. Порядок расторжения/прекращения действия Договора в связи с прекращением предоставления Электронных банковских услуг осуществляется в соответствии с условиями Договора и/или законодательством Республики Казахстан.

6. Процедуры безопасности в системе «Интернет-банкинг для юридических лиц»

13. В целях обеспечения конфиденциальности передаваемой и получаемой информации в Системе «Интернет-банкинг для юридических лиц» используется шифрование TLS (Transport Layer Security — безопасность транспортного уровня). Шифрование преобразует данные Клиента в Системе «Интернет-банкинг для юридических лиц» в зашифрованный код перед их отправкой через сеть Интернет и обеспечивает конфиденциальность информации Клиента на пути между компьютерной системой Банка и Интернет-браузером Клиента.
14. Клиент должен осуществить проверку браузера для определения возможности поддержки шифрования 256 bit.
15. TLS -протокол позволяет выявлять наличие искажений и/или изменений в содержании электронных документов, на основании которых Клиенту предоставляются Электронные банковские услуги.
16. В Системе «Интернет-банкинг для юридических лиц» используются межсетевые экраны (firewall/Brandmauer) для блокировки проникновения в компьютерные системы потенциально опасной информации и для предотвращения несанкционированного доступа к Системе «Интернет-банкинг для юридических лиц». Программное обеспечение межсетевых экранов может быть установлено на офисных и домашних компьютерах в качестве защиты от несанкционированного доступа и вирусов.
17. В целях защиты компьютера Клиента и информации о подключенных счетах Клиента к Системе «Интернет-банкинг для юридических лиц» Банк использует цифровые сертификаты, для проверки установления связи с Банком. При Идентификации Клиента и Аутентификации в Системе «Интернет-банкинг для юридических лиц» на веб-сайте Банка браузер Клиента запрашивает подтверждение веб-сайта Банка своей идентификационной информации посредством цифровых сертификатов. Браузер Клиента может проверить сертификат и предупредить Клиента, если данный веб-сайт не принадлежит Банку. При Идентификации Клиент обязан удостовериться в том, что данная проверка имела место быть.
18. Безопасность сеанса дистанционного банковского обслуживания обеспечивается в «защищенной» среде посредством шифрования Протоколом безопасных соединений (TLS). Технология TLS используется в рамках сеанса дистанционного банковского обслуживания для шифрования персональной информации Клиента, в целях сохранения конфиденциальности.
19. При предоставлении платежных услуг обмен информацией между Банком и Клиентом осуществляется посредством использования Устройства Digipass, генерирующего Сгенерированный код, так называемая динамическая идентификация Клиента.
20. В целях Идентификации Клиента при осуществлении доступа в Систему «Интернет-банкинг для юридических лиц» предусматриваются следующие идентифицирующие данные при входе в Систему: Логин Клиента, Логин пользователя, ПИН для входа в систему и Сгенерированный код, сгенерированный Устройством Digipass, назначенный/принадлежащий данному Пользователю/Уполномоченному лицу Клиента.
21. В целях Аутентификации при получении Клиентом платежных услуг предусматривается обязательное введение Сгенерированного кода, генерируемого Устройством Digipass.
22. Клиент не вправе разглашать/передавать третьим лицам Логин Клиента, Логин пользователя, ПИН для входа в систему, ПИН, Сгенерированный код, Устройство Digipass.
23. В целях безопасности в Системе «Интернет-банкинг для юридических лиц» предусмотрена функция отключения текущей сессии Клиента в Системе «Интернет-банкинг для юридических лиц». Под отключением текущей сессии Клиента в Системе «Интернет-банкинг для юридических лиц» понимается отказ в предоставлении Электронных банковских услуг в случае продолжительного (более 10 минут) отсутствия активных действий Клиента в Системе «Интернет-банкинг для юридических лиц» (неосуществление любых операций, не предоставление любых электронных документов и т.д.).

24. В целях подтверждения данных, указанных в Заявке, Банк вправе посредством телефонной связи получить/уточнить необходимые сведения, связанные с исполнением Заявки Клиента по номерам телефона, указанным Клиентом в Заявке.
25. При предоставлении электронных банковских услуг у Банка остается подтверждение об отправке и/или получении сообщений, на основании которых Клиенту предоставлены Электронные банковские услуги. Если иное не установлено Договором, подтверждение получения электронного сообщения производится путем направления подтверждения о его получении отправителю.
26. На основании надлежащим образом оформленного письма Клиента Банк предоставляет Клиенту подтверждение об отправке и/или получении Электронных банковских услуг, в течение не более 10 (десяти) рабочих дней с даты получения письма Клиента, в письменной форме способом, оговоренным в письме Клиента (посредством электронной почты/ Системы «Интернет-банкинг для юридических лиц»/нарочно/курьерской службы). Максимальные сроки оказания электронных банковских услуг, предоставляемых Банком в течение срока действия Договора, соответствуют срокам, предусмотренным законодательством Республики Казахстан.

(В раздел 6 внесены изменения согласно решению Правления от 05 июля 2017 года (протокол заседания №53).

6-1. Процедуры безопасности в системах «Интернет-банкинг для юридических лиц «ForteBusiness» и Мобильный интернет-банкинг «ForteBusiness»»

Глава дополнена понятием мобильный интернет-банкинг согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

27. В целях обеспечения конфиденциальности передаваемой и получаемой информации в Системе «ForteBusiness» используется шифрование TLS (Transport Layer Security – безопасность транспортного уровня). Шифрование преобразует данные Клиента в Системе «ForteBusiness» в зашифрованный код перед их отправкой через сеть Интернет и обеспечивает конфиденциальность информации Клиента на пути между компьютерной системой Банка и Интернет-браузером Клиента.
28. Клиент должен осуществить проверку браузера для определения возможности поддержки шифрования 256 bit.
29. TLS -протокол позволяет выявлять наличие искажений и/или изменений в содержании электронных документов, на основании которых Клиенту предоставляются Электронные банковские услуги.
30. В Системе «ForteBusiness» используются межсетевые экраны (firewall) для блокировки проникновения в компьютерные системы потенциально опасной информации и для предотвращения несанкционированного доступа к Системе «ForteBusiness». Программное обеспечение межсетевых экранов может быть установлено на офисных и домашних компьютерах в качестве защиты от несанкционированного доступа и вирусов.
31. В целях защиты компьютера Клиента и информации о подключенных счетах Клиента к Системе «ForteBusiness» Банк использует цифровые сертификаты, для проверки установления связи с Банком. При Идентификации Клиента и Аутентификации в Системе «ForteBusiness» на веб-сайте Банка браузер Клиента запрашивает подтверждение веб-сайта Банка своей идентификационной информации посредством цифровых сертификатов. Браузер Клиента может проверить сертификат и предупредить Клиента, если данный веб-сайт не принадлежит Банку. При Идентификации Клиент обязан удостовериться в том, что данная проверка имела место быть.
32. Безопасность сеанса дистанционного банковского обслуживания обеспечивается в «защищенной» среде посредством шифрования Протоколом безопасных соединений (TLS). Технология TSL используется в рамках сеанса дистанционного банковского обслуживания для шифрования персональной информации Клиента, в целях сохранения конфиденциальности.
33. При предоставлении платежных услуг обмен информацией между Банком и Клиентом осуществляется посредством использования Устройства Digipass, генерирующего Сгенерированный код, так называемая динамическая идентификация Клиента.
34. В целях Идентификации Клиента при осуществлении доступа в Систему «ForteBusiness» предусматриваются обязательно следующие идентифицирующие данные при входе в Систему: Логин пользователя, Пароль и Сгенерированный код, сгенерированный Устройством Digipass, назначенный/принадлежащий данному Пользователю/Уполномоченному лицу Клиента.
35. В целях Аутентификации при получении Клиентом платежных услуг предусматривается обязательное введение Сгенерированного кода, генерируемого Устройством Digipass.
36. Клиент не вправе разглашать/передавать третьим лицам Логин пользователя, Пароль, ПИН, Сгенерированный код, Устройство Digipass.
37. В целях безопасности в Системе «ForteBusiness» предусмотрена функция отключения текущей сессии Клиента в Системе «ForteBusiness». Под отключением текущей сессии Клиента в Системе «ForteBusiness» понимается отказ в предоставлении Электронных банковских услуг в случае

продолжительного (более 10 минут) отсутствия активных действий Клиента в Системе «ForteBusiness» (неосуществление любых операций, не предоставление любых электронных документов и т.д.).

38. В целях подтверждения данных, указанных в Заявке, Банк вправе посредством телефонной связи получить/уточнить необходимые сведения, связанные с исполнением Заявки Клиента по номерам телефонов, указанным Клиентом в Заявке.
39. При предоставлении электронных банковских услуг у Банка остается подтверждение об отправке и/или получении сообщений, на основании которых Клиенту предоставлены Электронные банковские услуги. Если иное не установлено Общими условиями, подтверждение получения электронного сообщения производится путем направления подтверждения о его получении отправителю.
40. На основании надлежаще оформленного письма Клиента, Банк предоставляет Клиенту подтверждение об отправке и/или получении Электронных банковских услуг, в течение не более 10 (десяти) рабочих дней с даты получения письма Клиента, в письменной форме способом, оговоренным в письме Клиента (посредством электронной почты/ Системы «ForteBusiness»/нарочно/курьерской службы). Максимальные сроки оказания электронных банковских услуг, предоставляемых Банком в течение срока действия Договора, соответствуют срокам, предусмотренным законодательством Республики Казахстан.
41. В целях обеспечения безопасности при работе в Системе «ForteBusiness» Пользователю необходимо следовать следующим правилам:

    1) устанавливать мобильное приложение и обновления к нему только из официальных онлайн магазинов приложения производителей мобильных операционных систем, находящихся в сети Интернет;

    2) не использовать нелицензионное, сомнительное, а также не проверенное на наличие вредоносных программ программное обеспечение;

    3) желательно использовать отдельный компьютер с ограниченным физическим доступом, исключительно для работы в Системе «ForteBusiness»;

    4) использовать лицензионное, своевременно обновляющееся антивирусное программное обеспечение. Действие вирусов может быть направлено на перехват идентификационной информации Пользователя;

    5) использовать современные операционные системы на своем компьютере и мобильном устройстве, с автоматическим своевременным обновлением, рекомендуемым компанией – производителем в целях устранения, выявленных в нем уязвимостей. Регулярно выполнять обновления операционной системы и браузера компьютера, что значительно повышает уровень безопасности;

    6) не подключать к компьютеру не проверенные на наличие вирусов внешние носители информации;

    7) для обеспечения дополнительной безопасности, при вводе пароля можно использовать «виртуальную клавиатуру», исключив тем самым возможность перехвата вводимых символов;

    8) не использовать устройства, подвергшиеся процессу модификации на системном уровне («рутированные», rootkit);

    9) не позволять кому-либо видеть набираемую на клавиатуре устройства комбинацию цифр пароля, Сгенерированного кода, сгенерированный Устройством Digipass, СМС-кода;

    10) при утере или краже мобильного телефона с зарегистрированным номером – заблокировать зарегистрированный телефонный номер через оператора мобильной связи и уведомить Банка о необходимости блокирования доступа к Системе «ForteBusiness»;

    11) после окончания работы закрывать окно Системы «ForteBusiness» с помощью кнопки «Выход» и никогда не оставлять компьютер или мобильное устройство с текущей сессией в Систему «ForteBusiness» без присмотра;

    12) не сохранять пароли в программах, устанавливающих Интернет-соединение, в текстовых файлах на компьютере либо на других электронных носителях информации, так как при этом существует риск его кражи и компрометации;
42. Банк не несет ответственность за:

    1) несанкционированный доступ к информации, составляющей банковскую тайну, возникший вследствие:

    – разглашения Пользователем Логина, ПИН для входа в Систему «ForteBusiness» и Сгенерированный код, сгенерированный Устройством Digipass, СМС –кода, необходимых для входа в Систему «ForteBusiness» и совершения операций;

    – утери или передачи Пользователем третьему лицу мобильного телефона или иного средства доступа к Системе «ForteBusiness»;

    2) несанкционированный доступ и операции с деньгами, размещенными на счетах, возникшие вследствие:

    – разглашения Пользователем Логина, ПИН для входа в систему и Сгенерированный код, сгенерированный Устройством Digipass, СМС –кода, необходимых для входа в Систему «ForteBusiness» и совершения операций;

    - утери или передачи Пользователем третьему лицу мобильного телефона или иного средства доступа к Системе «ForteBusiness»;

- несвоевременного обращения Пользователя в Банк для блокирования доступа к Системе «ForteBusiness»;
- перехвата Логина, ПИН для входа в Систему «ForteBusiness» и Сгенерированный код, сгенерированный Устройством Digipass, СМС –кода из-за несоблюдения Пользователями настоящих действий;
- ошибок, допущенных Пользователем при оформлении документов и указании неверных номеров счетов/телефонов и реквизитов;
- получения иными лицами информации о введенных Пользователем данных и проведенных операциях в результате перехвата каналов связи;
- оставлении Пользователем открытой сессии работы с Системой «ForteBusiness» без присмотра.

42-1. Для контроля целостности данных, Идентификации и Аутентификации Клиента применяются ключи ЭЦП, полученные клиентами в НУЦ РК. Порядок предоставления ключей и сертификатов ЭЦП регламентирован требованиями НУЦ РК. Для выполнения операций по работе с ЭЦП Мобильный интернет-банкинг использует библиотеки:

1) комплект разработчика НУЦ РК (NCALayer, Kalkan Crypt) - для формирования Хэша, формирования ЭЦП в подсистеме в Системе «Fortebusiness», а также проверки ЭЦП на сервере НУЦ;
2) ТУМАР-CSP - для формирования Хэша, формирования ЭЦП в мобильной версии Системы «Fortebusiness», а также проверки ЭЦП на сервере НУЦ.

Дополнен пунктом 42-1 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

42-2. В целях Идентификации и Аутентификации при использовании Мобильного интернет-банкинга предусматриваются следующие идентифицирующие данные: индивидуальный идентификационный номер, номер мобильного телефона (логин), Пароль, СМС-код, ЭЦП, биометрические данные, FaceID, TouchID, ПИН-код быстрого входа, принадлежащие Клиенту. В целях соблюдения Процедур безопасности, Пароль должен меняться Клиентом не реже 1 (одного) раза в 60 (шестьдесят) календарных дней.

Дополнен пунктом 42-2 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

42-3. В целях обеспечения безопасности в Мобильном интернет-банкинге предусмотрена функция автоматического отключения текущей сессии Клиента. Под автоматическим отключением текущей сессии Клиента в Мобильном интернет-банкинге понимается отказ в оказании электронных банковских услуг в случае продолжительного (более 3 (трёх) последовательных минут) отсутствия активных действий (неосуществление любых операций и действий и т.д.). Клиента в Мобильном интернет-банкинге. Банком могут быть предусмотрены дополнительные условия, требования для проверки подлинности, корректности, достоверности операций, совершаемых Клиентом и необходимые для оказания услуги, в целях повышения уровня безопасности от несанкционированных платежей, предотвращения мошеннических действий, недопущения разглашения конфиденциальной информации или иных противоправных действий.

Дополнен пунктом 42-3 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

42-4. Перед скачиванием мобильного приложения (Мобильный интернет-банкинг) в сервисах AppStore, PlayMarket, Клиенту предлагается ознакомиться с положениями Политики конфиденциальности (Приложение №2 к настоящим Правилам).

Дополнен пунктом 42-4 согласно решению и.о. Председателя Правления Нурумбет Ш.М. Заявка №2021-489998 от 10.11.2021 г.

(В раздел 6 Правил внесены дополнения согласно решению Операционного комитета от 16 мая 2019 года (протокол заседания №16).

(В раздел 6 Правил внесены дополнения согласно решению Правления № 01/2021-78 от 09.07.2021 года).

7. Заключительные положения

43. По вопросам, связанным с предоставлением Электронных банковских услуг Клиент может обратиться по следующим Контактным данным:

+7 (727) 258-40-40
+7 (727) 258-75-75
+7 (7172) 58-75-75
7575 с мобильного телефона
Факс: +7 (727) 259-67-87
E-mail: info@forte.bank
Адрес Банка: г. Нур-Султан, ул. Достык, 8/1

(В Пункт 27 внесены изменения согласно решению Правления от 05 июля 2017 года (протокол заседания №53).

44. Банк вправе в одностороннем порядке изменять Контактные данные с уведомлением Клиента о таких изменениях на веб-сайте Банка (www.forte.kz).
45. Банк вправе в одностороннем порядке вносить изменения в Правила предоставления электронных банковских услуг и своевременно размещать на соответствующем доступном для Клиента ресурсе Банка.
46. Иные вопросы, не урегулированные настоящими Правилами, разрешаются в соответствии с действующим законодательством Республики Казахстан, внутренними документами Банка, Договором и обычаями делового оборота, принятыми в банковской практике.

(В раздел 6 Правил внесены дополнения согласно решению Правления № 01/2021-78 от 09.07.2021 года).

ПРИЛОЖЕНИЕ №1

к Правилам предоставления электронных банковских услуг для юридических лиц/индивидуальных предпринимателей посредством систем «Интернет-банкинг для юридических лиц/ Интернет-банкинг для юридических лиц «ForteBusiness» и Мобильный интернет-банкинг «ForteBusiness»

Руководство э эксплуатации Устройства Digipass

Чтобы обеспечить высокий уровень защиты информации для клиентов, пользующихся системой «Интернет-банкинг для юридических лиц» / «ForteBusiness», в системе применяются устройства Digipass производства компании VASCO Data Security. Данная компания является мировым лидером среди производителей идентификационных устройств для систем, работающих в режиме on-line. Устройство Digipass 270 генерирует одноразовые (Сгенерированные) коды для входа в систему, а также для верификации документов.

1) Как пользоваться устройством Digipass 270

1.1) Как включить/выключить устройство?

Для включения устройства Digipass 270, надо одновременно нажать на кнопки и ◀. Для выключения устройства дважды нажмите на треугольную кнопку ◀. Устройство автоматически выключается через 30 секунд бездействия.

1.2) Как установить первоначальный PIN-код?

При первом использовании устройства Digipass 270 пользователь должен обязательно составить и запомнить персональный 5-значный PIN-код

Действие пользователя	Сообщение устройства Digipass
Включение устройства Digipass 270 и ◀	NEW PIN
Ввод персонального 5-значного PIN-кода	PIN CONF
Подтверждение нового PIN-кода (повторный ввод)	NEW PIN CONF APPLI _

1.3) Как изменить PIN-код?

В процессе использования устройства Digipass 270 текущий PIN-код может быть изменен.

Действие пользователя	Сообщение устройства Digipass
Включение устройства Digipass 270 и ◀	PIN
Ввод текущего PIN-кода и удерживание кнопки ◀ в течение нескольких секунд	APPLI _ NEW PIN
Ввод нового PIN-кода	PIN CONF
Подтверждение нового PIN-кода (повторный ввод)	NEW PIN CONF

1.4) Как сгенерировать одноразовый пароль?

Для входа в Систему Пользователь должен ввести в соответствующее поле свое Имя пользователя и сеансовый код, генерированный устройством Digipass 270.

Действие пользователя	Сообщение устройства Digipass
Включение устройства Digipass 270 и ◀	PIN
Ввод PIN-кода	APPLI _
Нажатие кнопки **1**	APPLI 1
Подтверждение нового PIN-кода (повторный ввод)	NEW PIN CONF

1.5) Строго запрещается вскрывать корпус устройства и подвергать иному воздействию!

2) Часто задаваемые вопросы

2.1) Что такое PIN-код?

PIN-код представляет собой комбинацию из **4/5** цифр, известную только Пользователю, владеющему данным устройством. Если PIN-код случайным образом становится известен третьим лицам, его надо незамедлительно сменить. В целях безопасности PIN-код должен быть максимально сложным. Его надо запомнить (не записывать) и не раскрывать третьим лицам.

2.2) Что делать, если введен неправильный PIN-код?

При неправильном вводе PIN-кода на экране появится сообщение ―FAIL X‖, где X – цифра от 1 до 5, указывающая количество неправильного ввода кода. Например, ―FAIL 3‖ означает, что PIN-код был 3 раза введен неправильно. Если PIN-код введен неправильно **5** раз подряд, на экране появляется сообщение ―LOCK PIN‖, и устройство блокируется. Для разблокировки устройства необходимо обратиться в Банк.

2.3) Что делать, если система не принимает число, генерированное устройством?

Если система не принимает число, генерированное устройством, вероятно, что устройство было заблокировано в банке в результате долгого бездействия, многоразового ввода неправильного PIN-кода или по иным причинам. Для разблокировки устройства необходимо обратиться в обслуживающий филиал Банка.

2.4) Что делать в случае утери устройства?

В случае утери устройства незамедлительно известите об этом Банк.

(В Приложение 1 к Правилам внесены изменения согласно решению Правления № 01/2021-78 от 09.07.2021 года).

ПРИЛОЖЕНИЕ №2

к Правилам предоставления электронных банковских услуг для юридических лиц/индивидуальных предпринимателей посредством систем «Интернет-банкинг для юридических лиц/ Интернет-банкинг для юридических лиц «ForteBusiness» и Мобильный интернет-банкинг «ForteBusiness»

Политика Конфиденциальности

АО «ForteBank» (далее по тексту — Банк) благодарит Вас за проявленный интерес к мобильному интернет - банкингу для юридических лиц «Fortebusiness» (далее по тексту — Система).

Защита персональных данных и иной информации клиента (далее по тексту - Пользователь) очень важна для Банка, поэтому мы с особым вниманием относимся к их защите, которые обрабатываются при использовании Системы.

Система позволяет Пользователю осуществлять взаимодействие с Банком в рамках заключенного(-ых) договора(-ов) банковского обслуживания. Получение доступа к использованию Системы означает безоговорочное согласие Пользователя с положениями настоящей Политики, в том числе согласие на сбор и обработку его персональных данных.

Банком обеспечивается безопасность персональных данных и иной информации, получаемых от Пользователя Системы. Настоящая Политика разработана с целью указания перечня персональных данных и иной информации, которые могут быть запрошены у Пользователя Системы, а также способов обработки Банком и иными лицами таких данных/информации. В настоящей Политике также указаны цели, для которых обрабатываются персональные данные и иная информация Пользователя.

Отдельными соглашениями с Пользователем могут быть предусмотрены иные цели, для которых требуется обработка персональных данных и иная информация Пользователя. В настоящей Политике также указаны основные меры предосторожности, которые должны предприниматься Пользователем для того, чтобы его персональные данные и иная информация оставались конфиденциальными.

1. При использовании Системы Банк может собирать, запрашивать и (-или) использовать/получать:

1.1. информацию о местонахождении Пользователя, геолокацию, точные координаты местонахождения, приблизительные координаты местонахождения Пользователя для поиска ближайших к Пользователю отделений Банка, банкоматов;
1.2. доступ к камере мобильного устройства Пользователя, доступ к медиатеке (фотогалерея/видео галерея) мобильного устройства Пользователя для создания фотодокументов, для создания и/или сохранения изображения и/или фото, для сохранения медиа-материалов, сохранение изображения на мобильном устройстве Пользователя, для отображения фотографии Пользователя в Сервисе, для загрузки необходимых документов;
1.3. информацию о Пользователе: ИИН/БИН, номер мобильного телефона, а также биометрические данные (в том числе Face ID, Touch ID) для первичной и последующей идентификации Пользователя в Системе;
1.4. доступ к файлам и к хранилищам данных мобильного устройства Пользователя, для целей загрузки сертификатов электронно-цифровой подписи (ЭЦП);
1.5. доступ к другим приложениям, установленным на мобильном устройстве Пользователя, в целях получения сгенерированного цифрового OTP-кода для подтверждения расходных операций в Системе;
1.6. доступ к состоянию мобильного устройства Пользователя, включая номер телефона мобильного устройства Пользователя, текущую информацию о сотовой сети мобильного устройства Пользователя, состояние всех текущих вызовов и список всех учетных записей, зарегистрированных на мобильном устройстве Пользователя для повышения уровня безопасности использования Системы, для автозаполнения номера мобильного телефона при идентификации в Системе, а также предоставления Пользователю электронных банковских услуг ;

1.7. информацию о мобильном устройстве. Банком собираются данные о мобильном устройстве Пользователя, такие как модель мобильного устройства, версия операционной системы, уникальные идентификаторы устройства;

1.8. доступ к SMS сообщениям на мобильном устройстве Пользователя для целей автозаполнения кода подтверждения, направленного Банком в виде SMS – сообщения для идентификации, а также подтверждения операции Пользователя;

1.9. информацию о совершаемых операциях. При совершении операций, Банком собираются данные о месте, времени и сумме совершенных операций, тип способа оплаты, данные о продавце и (или) поставщике услуг, описания причины совершения операции, если таковые имеются, а также иную информацию, связанную с совершением указанных выше операций. При использовании информации Пользователя Банк руководствуется настоящей Политикой, законодательством Республики Казахстан, в том числе Законом Республики Казахстан «О персональных данных и их защите», а также внутренними документами Банка.

2. Система обрабатывает персональные данные и иную информацию Пользователя необходимые для предоставления и оказания услуг Банка (исполнение договора с Пользователем).

3. В отношении персональных данных и иной информации Пользователя сохраняется ее конфиденциальность, кроме случаев добровольного предоставления Пользователем таких данных/информации для общего доступа неограниченному кругу лиц.

4. Банк вправе предоставлять персональные данные и иную информацию Пользователя своим аффилированным лицам, а также партнерам и иным компаниям, в целях, указанных выше, в соответствии с требованиями законодательства Республики Казахстан.

5. Банк обязуется принять меры для предотвращения несанкционированного доступа третьих лиц к персональным данным и иной информации Пользователя. Любая информация такого рода может быть предоставлена третьим лицам не иначе как в порядке, установленном законодательством Республики Казахстан, в том числе в соответствии с предоставленными Пользователем Банку согласиями.

6. В случаях, когда использование паролей, SMS-кодов предполагает передачу либо хранение Банком какой-либо конфиденциальной информации, Банк обязуется принять все необходимые и зависящие от Банка меры организационного и технического характера для предотвращения доступа третьих лиц к такой информации до передачи ее Пользователю, а также во время хранения указанной информации.

7. Пользователь должен хранить данные учетной записи, такие как логин и пароль, втайне от третьих лиц. Пользователь обязуется незамедлительно сообщать Банку о любом случае подозрения несанкционированного использования его учетной записи. Безопасность использования Системы также зависит от соблюдения Пользователем рекомендаций Банка.