ПАМЯТКА О МЕРАХ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В ДИСТАНЦИОННОЙ СИСТЕМЕ «АЛЕФ-BUSINESS» И МОБИЛЬНОЙ ВЕРСИИ ДИСТАНЦИОННОЙ СИСТЕМЫ «АЛЕФ-BUSINESS»

1. **Общие меры безопасности:**
   1.1. Для исключения Компрометации Вашей финансовой информации и хищения средств, **настоятельно рекомендуем** Вам:
   - хранить носители ключей (Смарт-ключи) в месте, недоступном посторонним лицам. Исключить хранение ключей на жёстком диске, в сетевых каталогах и прочих общедоступных ресурсах, либо использовать крипто-контейнеры;
   - ограничить доступ третьих лиц к автоматизированным рабочим местам (компьютерам) и мобильным устройствам, посредством которых осуществляется доступ к Дистанционным системам. По возможности рекомендуются использовать отдельный компьютер, мобильное устройство для работы в Дистанционных системах;
   - хранить в тайне ПИН-код Смарт-ключа, Идентификатор, Пароль, исключить их запись на стикерах, Смарт-ключах и т.п. Никому не сообщайте ПИН-код Смарт-ключа, Идентификатор, Пароль по телефону, даже работникам Банка;
   - использовать Смарт-ключ только во время работы в Системе «Алеф-Business», в остальное время извлекать Смарт-ключ из компьютера и помещать его в место хранения;
   - на ежедневной основе контролировать движение по счетам (путем просмотра выписок), операции по которым могут осуществляться посредством Дистанционных систем и при обнаружении подозрительных операций незамедлительно обращаться в Банк;
   - использовать только доверенные компьютеры с лицензионным программным обеспечением. Используйте только поддерживаемое производителем программное обеспечение, минимальные требования к которому определены Договором комплексного банковского обслуживания юридических лиц (за исключением кредитных организаций), индивидуальных предпринимателей и лиц, занимающихся частной практикой, в АО АКБ «Алеф-Банк».;
   - установить и своевременно обновлять на компьютере и мобильном устройстве антивирусное программное обеспечение (ПО). Не отключать антивирусное ПО на компьютерах, мобильных устройствах;
   - записать контактный телефон Банка 8(495) 411-77-47. Если вас просят связаться с Банком по другому номеру, это может означать попытку мошенничества.

   1.2. При утрате мобильного телефона или иного мобильного устройства, используемого с абонентским номером подвижной радиотелефонной связи, на который Банк направляет Одноразовые пароли и (или) на которое установлена Мобильная версия Системы «Алеф-Business» Вам следует **незамедлительно** обратиться к своему оператору сотовой связи для блокировки SIM-карты и в Отделение Банка для блокировки доступа к Дистанционным системам.

   1.3. При внезапном прекращении работы SIM-карты необходимо **незамедлительно** обратиться к своему оператору сотовой связи за уточнением причин – в отношении Вас возможно проведение мошеннических действий третьими лицами.

   1.4. Будьте внимательны – не оставляйте свой телефон/устройство без присмотра, чтобы исключить несанкционированное использование Одноразовых паролей и (или) Мобильной версии Системы «Алеф-Business».

   1.5. Не устанавливайте на мобильный телефон или на устройство, на которое Банк направляет Одноразовые пороли и (или) на котором установлена Мобильная версия Системы «Алеф-Business», приложения по ссылкам, полученным от неизвестных Вам источников. **Помните, что Банк не рассылает своим Клиентам** ссылки или указания на установку приложений через SMS/MMS/e-mail-сообщения.

   1.6. Используйте только надежные и проверенные точки Wi-Fi. Не рекомендуется подключаться к популярным и/или бесплатным точкам доступа Wi-Fi, если Вы не уверены в достоверности имени точки доступа. Обращаем Ваше внимание, что точки доступа Wi-Fi, для подключения к которым не

требуется ввод пароля, могут представлять повышенную опасность в связи с возможными действиями мошенников, направленными на получение доступа к Вашим персональным данным.

2. **Обеспечение безопасности Идентификатора, ПИН-кода Смарт-ключа или Пароля, Одноразовых паролей, используемых при работе в Дистанционных системах:**

2.1. Вход в Дистанционные системы осуществляется путем ввода Идентификатора и ПИН-кода Смарт-ключа или Пароля. **Никакой иной информации для входа в систему вводить не требуется.**

Если при входе в Дистанционную систему Вам предлагается ввести любую иную персональную информацию или дополнительные сведения (номера банковских счетов, номер мобильного телефона или другие данные), **это указывает на мошенничество**! В данном случае необходимо немедленно прекратить сеанс работы в Дистанционной системе и срочно обратиться в Банк.

2.2. При получении от Банка Одноразового пароля (SMS-сообщения или PUSH-уведомления) на номер мобильного телефона/мобильное устройство **внимательно ознакомьтесь с информацией в сообщении/уведомлении**: все реквизиты операции в направленном Вам сообщении/уведомлении должны соответствовать той операции, которую Вы собираетесь совершить. Только после того как Вы убедились, что информация в этом SMS-сообщении/PUSH-уведомлении корректна, можно вводить Одноразовый пароль.

2.3. Банк **никогда не запрашивает** Одноразовые пароли **для отмены** операций или шаблонов в Дистанционной системе. Если Вам предлагается ввести Одноразовый пароль для отмены операции, в том числе и той, которую Вы не совершали, Вам необходимо прекратить сеанс работы в Дистанционной системе и срочно обратиться в Банк.

2.4. **Ни при каких обстоятельствах не сообщайте свои Одноразовые пароли никому, включая работников Банка.** Помните, что, вводя Одноразовый пароль, Вы даёте Банку право и указание провести операцию с указанными в SMS-сообщении/PUSH-уведомлении реквизитам.

3. **Обеспечение защиты устройств, которые Вы используете для доступа к Системе «Алеф-Business»**

- проверяйте, что веб-адрес Системы «Алеф-Business» в адресной строке начинается с «**https**». В ином случае не входите в Дистанционную систему;
- используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением;
- регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ;
- своевременно устанавливайте обновления операционной системы, рекомендуемые компанией-производителем;
- используйте дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты вашего устройства
- используйте персональные межсетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет, программы поиска шпионских компонент, программы защиты от «СПАМ» - рассылок и пр.;
- включите системный аудит событий;
- используйте встроенные средства блокировки и разблокировки компьютера (логин/пароль для входа в операционную систему компьютера).
- не используйте мобильное устройство для доступа к Системе «Алеф-Business», для этого существует Мобильная версия Системы «Алеф-Business».

Завершение работы с Системой «Алеф-Business» выполняйте путем выхода, используя соответствующий пункт меню.

4. **Обеспечение защиты устройств, которые Вы используете для доступа к Мобильной версии Системы «Алеф-Business»:**

- подключайте к услугам Банка номера телефонов, которые принадлежат только Вам;
- используйте только официальные Мобильные приложения Банка, доступные в официальных магазинах приложений производителей мобильных платформ (App Store и Google Play);
- своевременно устанавливайте доступные обновления операционной системы и приложений на Ваше мобильный устройство;

- используйте антивирусное программное обеспечение для мобильного устройства, своевременно устанавливайте на него обновления антивирусных баз.
- не устанавливайте на свой мобильный телефон/устройство нелицензионные операционные системы, так как это отключает защитные механизмы, заложенные производителем мобильной платформы. В результате Ваш телефон становится уязвимым к заражению вирусными программами;
- не переходите по ссылкам и не устанавливайте приложения/обновления безопасности, пришедшие в SMS-сообщении, PUSH-уведомлении или по электронной почте, в том числе от имени Банка;
- не указывайте номер мобильного телефона, использующийся для получения Одноразовых паролей, в социальных сетях и других открытых источниках;
- используйте встроенные средства блокировки и разблокировки мобильного устройства (PIN-код/биометрические данные для разблокировки мобильного устройства).

Завершайте работу с Мобильной версией Системы «Алеф-Business», используя кнопку «Выход».

5. **Просим Вас незамедлительно обращаться в Отделение Банка при возникновении следующих ситуаций:**
   5.1. На компьютере, мобильном устройстве, используемом для работы в Дистанционных системах, обнаружено вредоносное программное обеспечение (вирусы, «трояны» и т.д.).
   5.2. В «Журнале сеансов работы» обнаружены факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время).
   5.3. В выписках по счетам обнаружены несанкционированные Вами расходные операции.
   5.4. Вы не можете получить доступ к Системе ДБО «Алеф-Business» по неизвестным причинам.
   5.5. Смена номера мобильного телефона, использующегося для получения Одноразовых паролей.
   5.6. Утерян Смарт-ключ, мобильное устройство, использующееся для получения Одноразовых паролей и (или) для работы в мобильной версии Системы «Алеф-Business» либо у Вас возникло подозрение о доступе к ним со стороны третьих лиц.