Приложение № 1
к Регламенту обслуживания клиентов -
физических лиц с использованием системы
дистанционного банковского обслуживания
«iBank»

Правила пользования Системой ДБО

1. Ограничения способов и мест использования Системы ДБО.

Для доступа в Систему ДБО необходим персональный компьютер или мобильное устройство, подключенное к сети Интернет, с установленным на нем современным интернет-браузером: Microsoft Internet Explorer, Mozilla Firefox, Opera, Google Chrome, Safari.

Предоставление информации по Счетам / Платежным картам Клиента, открытым в Банке, / заключение договоров может быть невозможно в связи с техническими ограничениями, связанными с проведением Регламентных работ на стороне Банка. О наличии таких ограничений Банк уведомляет Клиента путем размещения сообщений на официальном сайте Банка и в Системе ДБО.

2. Случаи повышенного риска, связанные с использованием Системы ДБО.

Клиент соглашается на подключение к Системе ДБО, осознавая, что сеть Интернет не всегда является безопасным каналом связи и передачи информации, и осознает риски, связанные с возможным нарушением конфиденциальности, и иные риски, возникающие вследствие использования такого канала доступа.

Банк информирует Клиента о следующих случаях повышенного риска, связанных с использованием Системы ДБО посредством доступа с персонального компьютера, которых Клиент должен избегать / принимать усиленные меры для обеспечения режима конфиденциальности:

- использование Системы ДБО с персонального компьютера, размещенного в общественном месте. В случае необходимости такого использования Клиент должен максимально обезопасить себя, выполнив условия обеспечения безопасности соединения в сети Интернет и использования Средств доступа;
- кража или потеря мобильного телефона, на номер которого приходят SMS-сообщения с Кодами подтверждения для формирования ЭД посредством Системы ДБО или который используется для доступа в Систему ДБО. В случае подозрения на кражу или потерю мобильного телефона Клиент обязан незамедлительно обратиться в Банк для временной блокировки доступа в Систему ДБО (до восстановления SIM-карты) или изменения номера мобильного телефона;
- невыполнение условий обеспечения безопасности автоматизированного рабочего места (далее - АРМ), с которого осуществляется доступ в Систему ДБО;
- получение доступа в Систему ДБО посредством браузера с устройства, содержащего вредоносный или модифицированный код, а также с устройств, на которых произведена модификация системы с целью получения доступа к файловой системе или иных прав, не предусмотренных разработчиками операционной системы.

Банк информирует Клиента о недопустимости ввиду повышенного риска использования для получения доступа в Систему мобильного устройства, которое:

- может содержать вредоносный или модифицированный код;

– может содержать не предусмотренное разработчиками и/или не сертифицированное производителем мобильного устройства программное обеспечение;

– прошло модификацию Системы, не предусмотренную разработчиками программного обеспечения и/или не сертифицированную производителем мобильного устройства.

3. Меры обеспечения безопасности при использовании Системы ДБО.

Клиент обязан исключить доступ третьих лиц к Паролю и Логину:

– не записывать Пароль и Логин, в том числе совместно;

– не сохранять информацию о Средствах доступа в памяти браузера;

– держать в тайне и не передавать третьим лицам (в том числе государственным органам) информацию о Средства доступа и Кодах Подтверждения;

– незамедлительно обратиться в Банк для смены Пароля в случае появления подозрений в том, что Пароль мог оказаться известен третьим лицам;

– в случае передачи (списания, утилизации и т.п.) сторонним лицам стационарного компьютера, ноутбука или мобильного устройства, на котором ранее была установлена Система ДБО, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности Клиента.

Клиент должен обеспечить безопасность соединения в сети Интернет между компьютером Клиента и сервером Банка (при доступе с персонального компьютера, если не указано иное), работа должна осуществляться в защищенном режиме:

– собственноручно набирать в адресной строке браузера адрес Системы ДБО, либо переходить по ссылке, размещенной на официальном сайте Банка;

– не переходить на адрес Системы ДБО по ссылкам, размещенным в электронных письмах или размещенным на сайтах в сети Интернет (кроме официального сайта Банка);

– после входа на стартовую страницу Системы ДБО удостовериться, что соединение установлено по протоколу HTTPS (в адресной строке указана аббревиатура https://)

– при подключении к сайту ДБО проверить подлинность сертификата сайта Системы ДБО (наличие значка защищенного соединения – замочка – в правом нижнем углу или в адресной строке браузера).

Клиент должен обеспечить безопасность АРМ и мобильного устройства, с которого осуществляется доступ в Систему ДБО:

– использовать на АРМ и мобильном устройстве только лицензионное программное обеспечение;

– для доступа с мобильного устройства Клиент должен использовать приложение, полученное только через официальный ресурс распространения программного обеспечения для мобильных устройств;

– использовать АРМ и мобильное устройство, на котором установлена только одна операционная система;

– работать в операционной системе АРМ под локальной учетной записью с ограниченными правами доступа, работа с административными привилегиями у пользователя операционной системы повышают вероятность проникновения вредоносного программного обеспечения;

- не использовать на мобильных устройствах модифицированные или измененные операционные системы;
- установить на АРМ специальные лицензионные программные и аппаратные средства защиты (межсетевые экраны (firewall), лицензионное антивирусное программное обеспечение, лицензионные средства обнаружения вредоносных программ), и следить за их своевременным обновлением;
- производить регулярное обновление лицензионного программного обеспечения, установленного на АРМ и мобильном устройстве;
- запускать на АРМ и мобильном устройстве программы, полученные только из доверенных источников (особую опасность могут представлять программы, полученные по электронной почте или из сети Интернет);
- файлы, полученные из общедоступных сетей передачи данных, не рекомендуется открывать и использовать без проведения соответствующих проверок для исключения программных закладок и вирусов;
- установить парольную защиту на вход в АРМ и мобильное устройство;
- регулярно (один раз в три месяца) проводить смену Пароля,
- мобильное приложение Банка необходимо удалять с телефона в том случае, если планируется продажа устройства, передача его в ремонт и т. д.

При изменении Пароля рекомендуется придерживаться следующих правил:

- длина Пароля – не менее 8 символов;
- Пароль не должен совпадать ни с одним из последних трех Паролей, ранее использованных Клиентом;
- Пароль не должен совпадать с Логином;
- в Пароле должны присутствовать символы из разных регистров (большие и маленькие буквы) и цифры. Для предотвращения возможных осложнений, связанных с различной кодировкой, рекомендуется использовать «латиницу»;
- Пароль не должен целиком состоять из комбинации символов, несущей смысловую нагрузку. Не рекомендуется использовать имена, названия, общепринятые аббревиатуры, адреса или другие общеизвестные слова и их сочетания, в том числе русское слово, набранное в латинской транскрипции (например: ПОЕЗД - GJTPL);
- последовательность символов Пароля не должна иметь очевидных закономерностей (например: Пароли a1a2a3a4, 1111111a, 12367890, ASDFGHJK имеют очевидные зависимости между своими символами).

Дополнительные рекомендации по безопасности при использовании программного обеспечения Системы ДБО, предназначенного для установки на мобильные устройства (мобильного приложения), размещены на сайте Банка.