Приложение № 2

Обязательства клиента
по выполнению правил безопасной работы при использовании клиентской части Системы ДБО

В соответствии с Договором ДБО Клиент подтверждает, что для обеспечения безопасной работы в Системы ДБО обязуется:

- обеспечить защиту от несанкционированного доступа к Клиентскому рабочему месту (АРМ Клиента), защиту от несанкционированного доступа и сохранность Ключей ЭП, Логинов и Паролей для входа в Систему ДБО, защиту от несанкционированного доступа к Мобильному устройству с активированным Мобильным приложением PayControl и Мобильным приложением Банка, а также защиту от несанкционированного доступа к другой конфиденциальной информации;
- в случае использования канала «Интеграционный Клиент-Банк» обеспечить защиту от несанкционированного доступа в Систему ДБО через рабочие места Клиента, которые участвуют в обмене ЭД с Банком, а также выполнение иных требований, установленных настоящим Приложением, на стороне Клиента;
- незамедлительно информировать Банк любым доступным способом обо всех случаях невозможности расшифровки ЭД, отрицательного результата проверки подлинности ЭП, нештатной работы Системы ДБО, неполучения информационных сообщений Банка;
- соблюдать следующие организационные меры:

☑ **Требования к сохранности Пароля/ Пароля к Ключу Серверной ЭП:**

– Пароль выбирается самостоятельно;

– если Пароль записан на бумаге, то хранится в месте, недоступном для неуполномоченных лиц, рекомендуется использовать надёжные металлические хранилища, оборудованные внутренними замками;

– запрещено записывать Пароль на съёмный носитель, монитор, клавиатуру и пр.;

– Пароль должен содержать не менее 8 различных символов (буквы, цифры, большой / малый регистр, спецсимволы);

– в качестве Пароля не должны быть использованы: ИНН и другие реквизиты Клиента, имена и фамилии, последовательности, состоящие из повторяющихся или одних цифр (в том числе номера телефонов, памятные даты, номера автомобилей и прочее, что можно связать с Клиентом);

– при Компрометации / подозрении на Компрометацию Пароля следует незамедлительно уведомить об этом Банк в соответствии с разделом Порядок действий при Компрометации / подозрении на Компрометацию настоящего Приложения;

– рекомендуемая периодичность смены пароля – не реже 1 (одного) раза в 3 (три) месяца.

☑ **Правила хранения и использования Ключевых носителей:**

– для хранения USB-Токенов необходимо использовать надёжные металлические хранилища, оборудованные внутренними замками, для исключения возможности несанкционированного доступа к ним неуполномоченных лиц;

– запрещается извлекать из хранилища носители с Ключами ЭП, если они не используются для работы с Системой ДБО;

– никогда не передавать Ключи ЭП третьим лицам для проверки работы Системы ДБО, проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок Уполномоченное лицо Клиента должно лично подключить носитель к

рабочей станции, убедиться, что пароль доступа к ключу вводится в интерфейс Системы ДБО, и лично ввести Пароль, исключая возможность его Компрометации;

– запрещается передавать Ключевые носители третьим лицам, оставлять без присмотра, а также (предпринимать попытки по проведению записи) записывать на USB-Токен постороннюю информацию;

– запрещается снятие несанкционированных копий с Ключевого носителя;

– при Компрометации / подозрении на Компрометацию среды исполнения (наличие в компьютере вредоносных программ), а также атрибутов доступа к Мобильному устройству (Логин, Пароль, графический ключ, PIN-код и т.д.) следует незамедлительно уведомить об этом Банк в соответствии с разделом Порядок действий при Компрометации / подозрении на Компрометацию настоящего Приложения;

– по требованию работника технической поддержки Системы ДБО в случае подозрения на Компрометацию выполнить антивирусную проверку АРМ Клиента;

– оказывать содействие Банку в установлении фактов несанкционированного доступа к Системе ДБО и Компрометации. Обеспечивать доступ работников Банка к техническим средствам, на которых установлена клиентская часть Системы ДБО для проведения работ по её установке и сопровождению;

☑ **Требования к выпуску и хранению API-токена при взаимодействии посредством API Интеграция в рамках канала «Интеграционный Клиент-Бак»:**

– выпустить API-токен в Системе iBank для Уполномоченных лиц, от имени которых будут формироваться запросы к API Интеграция;

– установить срок действия API-токена при его создании (по умолчанию 365 дней));

– срок действия API-токена может быть ограничен Банком исходя из срока действия полномочий Уполномоченного лица;

– в случае утери значения API-токена или изменения IP-адреса (если в процессе создания API-токена указывались IP-адреса) на стороне Клиента необходимо создание нового API-токена;

– запрещается передавать API-токен третьим лицам.

☑ **Соблюдение требований по обеспечению безопасности Ключевой информации:**

– все отчуждаемые (внешние) Ключевые носители должны учитываться поэкземплярно в специальных журналах согласно установленной нормативными актами Российской Федерации форме;

– учёт и хранение носителей СКЗИ, учёт Ключевых носителей должны быть поручены специально назначенным работником. Каждый владелец ЭП несёт персональную ответственность за его использование и сохранность;

– поэкземплярный учёт сформированных Уполномоченными лицами Клиента криптографических ключей осуществляется Клиентом;

– хранение Ключевых носителей допускается в одном хранилище с другими документами при условии, исключающем их непреднамеренное разрушение или уничтожение;

– Уполномоченными лицами или по поручению руководителя организации одним из работников из числа допущенных к эксплуатации СКЗИ, должен проводиться периодический контроль сохранности входящего в состав СКЗИ оборудования, а также всего используемого программного обеспечения для предотвращения внесения программно-аппаратных закладок и вредоносного программного обеспечения.

☑ **Правила хранения и использования Устройств подтверждения:**

– для хранения Устройств подтверждения необходимо использовать надёжные металлические хранилища, оборудованные внутренними замками, для исключения возможности несанкционированного доступа к нему неуполномоченных лиц и повреждение материального носителя;

– не извлекать из хранилища Устройство подтверждения, если оно не используются для работы с Системой ДБО;

– не раскрывать третьим лицам информацию об Устройстве подтверждения, находящемся в его распоряжении;

– не передавать его в пользование лицам, не являющимся Уполномоченными лицами Клиента, для распоряжения денежными средствами, находящихся на Счёте, или в иных целях, оставлять Ключевые носители без присмотра;

– в случае утраты или поломки Устройства подтверждения необходимо уведомить об этом Банк в соответствии с разделом Порядок действий при Компрометации / подозрении на Компрометацию настоящего Приложения.

☑ **Ограничение доступа и требования к рабочим местам, с которых осуществляется работа с Системой ДБО:**

– право доступа предоставляется только уполномоченным лицам, непосредственно осуществляющим работу с Системой ДБО. Исключить доступ к компьютерам неуполномоченных лиц, не имеющих отношения к работе с Системой ДБО;

– запрещается установка программных средств, не предназначенных для выполнения служебных обязанностей Уполномоченных лиц Клиента, допущенных к работе с Системой ДБО;

– применять на рабочем месте лицензионные ПО (операционные системы, офисные пакеты и пр.), лицензионные средства антивирусной защиты, обеспечить возможность регулярного автоматического обновления антивирусных баз;

– работа с Системой ДБО немедленно прекращается при подозрении, что компьютер заражен, а также в случае обнаружения незарегистрированных программ или нарушения целостности операционной системы – обязательно уведомить об этом Банк в соответствии с разделом Порядок действий при Компрометации / подозрении на Компрометацию настоящего Приложения;

– для работы в Системе ДБО крайне не рекомендуется выбирать переносной компьютер (ноутбук). Если Клиентом выбран ноутбук, запрещается подключать ноутбук к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.д.);

– в случае передачи (списание, выброс, ремонт) сторонним лицам компьютера (ноутбука), на котором ранее была установлена Система ДБО, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу Клиента, в том числе следы работы в Системе ДБО;

– использовать дополнительное программное обеспечение, позволяющее повысить уровень защиты компьютера – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «спам»–рассылок и пр.;

– включить автоматическую блокировку экрана после ухода уполномоченного лица с рабочего места.

☑ **Соблюдение правил безопасной работы в сети интернет на рабочих местах Системы ДБО:**

– не открывать сайт Системы ДБО по ссылкам (особенно баннерным или полученным через электронную почту);

– не отвечать на подозрительные письма с просьбой выслать авторизационные и другие конфиденциальные данные;

– на компьютерах, используемых для работы с Системой ДБО, исключить посещение интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного ПО и т.п.;

– не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях;

– на компьютере запрещено запускать программы, полученные из ненадежных источников;

– если Клиент эксплуатирует выделенный высокоскоростной канал доступа в сеть интернет, ограничить диапазон IP-адресов, с которых разрешён доступ к Системе ДБО с использованием Ключей ЭП, зарегистрированных Банком по Заявлению, переданному Клиентом в Банк;

–обращать внимание на любые изменения в привычных процессах установления соединения с Системой ДБО или в функционировании Системы ДБО. При возникновении любых сомнений в правильности функционирования Системы ДБО незамедлительно обратиться в Банк по телефону службы технической поддержки, указанному на официальном сайте Банка в сети Интернет www.abr.ru;

–в случае появления предупреждений Браузера о перенаправлении Клиента на другой сайт при подключении к Системе ДБО Банка, отложите совершение операций и обратитесь в службу поддержки Банка по телефону службы технической поддержки, указанному на официальном сайте Банка в сети Интернет www.abr.ru.

☑ **Требования к сотрудникам Клиента:**

– Клиент обязан назначить Приказом уполномоченных лиц по работе с Системой ДБО, утвердить соответствующие должностные инструкции, исключить доступ к компьютерам неуполномоченных лиц, не имеющих отношения к работе с Системой ДБО;

– при регистрации в Системе ДБО в соответствии с разделом **Ошибка! Источник ссылки не найден.** настоящих Правил, руководствоваться Инструкцией по установке Системы ДБО;

– каждое уполномоченное лицо, имеющее доступ к Ключевым носителям, паролям и другой конфиденциальной информации, должно быть проинформировано об ответственности за разглашение конфиденциальной информации;

– при обслуживании компьютера Уполномоченного лица Клиента, на котором используется Система ДБО, третьими лицами – обеспечивать контроль над выполняемыми ими действиями;

– при увольнении Уполномоченного лица, имевшего доступ к Ключу ЭП, обязательно проинформировать об этом Банк в целях блокировки Банком Ключа ЭП/ Ключа PayControl;

– при увольнении Уполномоченного лица Клиента, имевшего технический доступ к секретному Ключу ЭП/ Ключу PayControl, обязательно проинформировать об этом Банк в целях блокировки Банком Ключа ЭП/ Ключа PayControl;

– при увольнении Уполномоченного лица, осуществлявшего обслуживание рабочей станции, используемой для работы с Системой ДБО, принять меры для обеспечения отсутствия вредоносных программ на компьютерах;

– при наличии Счёта в Банке:

- контролировать актуальность Номеров телефонов для направления Кодов подтверждения/SMS-сообщений/PUSH-сообщений, а в случае их изменения – незамедлительно информировать о таком изменении Банк по форме Заявления об изменении данных;

- информировать Уполномоченных лиц о недопущении ситуаций переполнения памяти Мобильных устройств, что может являться препятствием для приёма SMS-сообщений Банка с Кодами подтверждения/ PUSH-сообщений, а также о необходимости исключить передачу мобильного телефона, который используется для получения SMS-сообщений Банка, третьим лицам;
- в случае утраты телефона, на который приходят Коды подтверждения /SMS-сообщения/PUSH-сообщения, обеспечить немедленную блокировку номера телефона у оператора сотовой связи;
- информировать Банк о смене телефонного номера и SIM-карты Мобильного устройства, используемого для получения SMS-сообщений с Кодами подтверждения/ PUSH-сообщений от Банка;
- при поступлении на телефон Уполномоченного лица SMS-сообщений/ PUSH-сообщений, свидетельствующих о попытке входа в Систему ДБО или подтверждения отправки документов, которых данное лицо не совершало, немедленно уведомить об этом Банк в соответствии с разделом Порядок действий при Компрометации / подозрении на Компрометацию настоящего Приложения.

☑ **Требования по обеспечению безопасности использования Клиентом Мобильного устройства с Мобильным приложением PayControl, Мобильным приложением Банка.**

– мобильное устройство, предназначенное для использования Клиентом с Мобильным приложением PayControl, Мобильным приложением Банка, должно быть приобретено у официального продавца и быть сертифицировано по требованиям ГОСТ в соответствии с действующим законодательством для использования на территории Российской Федерации;

– мобильное устройство Клиента имеет поддерживаемую Мобильным приложением PayControl и Мобильным приложением Банка лицензионную версию операционной системы:

a) Android 5.0 и выше;
b) iOS 10.X и выше.

–не использовать Мобильное приложение PayControl и Мобильное приложение Банка на Мобильных устройствах с расширенными правами (Jailbreak, Root или иные операции, не поддерживаемые официально производителями);

– для операционной системы Мобильного устройства и приложений, установленных на Мобильное устройство, Клиентом установлены максимально возможные на текущее время обновления, рекомендованные производителем/разработчиком;

– мобильное приложение PayControl самостоятельно установлено Клиентом из одного из авторизованных магазинов приложений (AppStore или PlayМаркет для iOS/Android соответственно). Клиент не использовал переход к указанным сервисам и не совершал установку Мобильного приложения PayControl по ссылке из других источников;

– если при установке Мобильного приложения PayControl появились сообщения о необходимости удаления приложения/приложений, представляющих угрозу для Мобильного приложения PayControl, необходимо удалить представляющие угрозу приложение/приложения с Мобильного устройства.

1. для разблокировки Мобильного устройства использовать максимально возможный из доступных на данном Мобильном устройстве способ защиты от несанкционированного доступа к функциям устройства и хранящихся на нём данным (в порядке убывания стойкости защиты):

a) средство распознания радужной оболочки глаза;
b) средство распознавания отпечатка пальца или лица (TouchID, FaceID);
c) пароль длиною не менее 6 символов (включая буквы и цифры);
d) графический ключ;

e) PIN-код.

При использовании пароля или PIN-кода Клиент запомнил их и не сохранил в памяти Мобильного устройства.

– мобильное устройство настроить на автоматическую блокировку устройства по истечении определённого времени (не более 5 (пяти) минут);

– на Мобильном устройстве под управлением ОС Android используется средство защиты от вредоносного кода («антивирусное программное обеспечение»);

– на Мобильном устройстве под управлением ОС Android отключить возможность установки приложений из непроверенных источников;

– мобильное устройство с Ключами инициализации PayControl (направляются/передаются Банком каждому УЛ Клиента: QR-код + код в SMS-сообщении) и самостоятельно выработанными УЛ Клиента Ключами ЭП на основе средства PayControl, а также атрибуты доступа к Мобильному устройству (Логин, Пароль, графический ключ, PIN-код) никогда не передаётся Клиентом неуполномоченным лицам, включая руководство организации, коллег и членов семьи Уполномоченного лица Клиента и не оставляется им без присмотра;

– мобильное устройство, с установленным Мобильным приложением PayControl, использовать только для посещения сайтов и установки приложений, необходимых и достаточных Клиенту для ведения его коммерческой/уставной деятельности;

2. мобильное устройство не подключать к компьютерам, безопасность которых Клиент не может гарантировать, а именно:

a) обеспечение доверенной среды;

b) отсутствие удалённого управления;

c) отсутствие установленных/запущенных вредоносных программ.

3. мобильное устройство не подключать к общественным WI-FI сетям. Общественные WI-FI сети, как правило, плохо защищены, их настройки неизвестны;

4. никогда и никому не сообщать Пароль для Аутентификации при входе в Мобильное приложение PayControl и Мобильное приложение Банка;

–обеспечить использование Ключей PayControl в Системе ДБО только УЛ Клиента (с установленными правами подписи);

–в случае возникновения вопросов по работе в Системе ДБО с Мобильным приложением PayControl и Мобильным приложением Банка обратиться в службу поддержки Банка по телефону службы технической поддержки, указанному на официальном сайте Банка в сети Интернет www.abr.ru.

☑ **Дополнительные рекомендации для владельцев смартфонов:**

– установить на вашем Мобильном устройстве и регулярно обновлять мобильный антивирус (рекомендуется использовать антивирус российского производителя, так как он учитывает региональную специфику вредоносного ПО);

– своевременно устанавливать обновления для вашего Мобильного устройства и установленных на нём приложений. Установку производить только из авторизованных магазинов приложений (AppStore или PlayМаркет для iOS/Android соответственно, маркетов производителей устройств и т.п.). Иные способы установки приложений и обновлений небезопасны. Недопустима установка или обновление приложений по ссылке в e-mail / SMS-сообщении от имени Банка. Обратите внимание: Банк никогда не высылает писем и SMS-сообщений с прямыми ссылками на установку или обновление приложений;

– при установке на ваше Мобильное устройство дополнительного программного обеспечения обращайте внимание на полномочия, которые необходимы программе. Не допускать установки программ, которым требуются излишние полномочия, особенно в части чтения и отправки SMS-сообщений, доступа к сети Интернет, клавиатуре

и т.п. При наличии технической возможности рекомендуется включить на Мобильном устройстве режим установки только подписанных приложений с проверкой сертификата;

– если Вы заметили, что на ваше Мобильное устройство перестали приходить SMS-сообщения, в том числе перестали приходить Коды подтверждения/ PUSH-сообщения от Банка, необходимо прекратить использование Мобильного устройства. В данном случае возможно мошенничество с заражением вашего Мобильного устройства вирусом, перехватывающим SMS-сообщения. Для проверки рекомендуем установить SIM-карту в другое мобильное устройство, провести операцию в Системе ДБО и дождаться прихода Кода подтверждения/ PUSH-сообщения. Так же о заражении вирусом может свидетельствовать подозрительная работа устройства (самопроизвольные звонки и рассылки SMS-сообщений, несанкционированная загрузка и установка программного обеспечения). В случае выявления данных фактов рекомендуем обратиться за помощью в службу технической поддержки производителя Вашего мобильного устройства.

☑ **Порядок действий при Компрометации / подозрении на Компрометацию**

– Клиенту в целях информирования Банка о наступлении события Компрометации или подозрения о Компрометации в день выявления факта Компрометации/ подозрения о Компрометации необходимо оповестить об этом Банк по телефону службы технической поддержки Системы ДБО, указанному на официальном сайте Банка в сети Интернет www.abr.ru в разделе «Вход в Интернет-Банк» (окно входа в Систему ДБО).

Устное обращение по телефону службы технической поддержки Системы ДБО о временной блокировке скомпрометированного Ключа ЭП (УНЭП, УКЭП) / приостановлении использования Системы ДБО должно быть подтверждено письменным Заявлением о компрометации (Приложение № 11 к Правилам), форма которого размещена на официальном сайте Банка (www.abr.ru). Подать Заявление о компрометации в Банк можно способами, определёнными подп. **Ошибка! Источник ссылки не найден.** Правил, либо на бумажном носителе, подписанным Представителем Клиента и заверенным печатью (при наличии) по месту нахождения отделения Банка, либо по Системе ДБО (при наличии у Клиента нескомпрометированных Ключей ЭП) в формате ЭСИД «Письмо».

– При информировании Банка по телефону службы технической поддержки Системы ДБО:

- Представитель Клиента (заявитель) сообщает наименование Клиента (владельца Счёта), свои ФИО и должность, а также ФИО и должность Уполномоченного лица Клиента, в отношении которого выявлены события Компрометации или подозрения на Компрометацию;
- Банк по факту обращения представителя Клиента (заявителя) незамедлительно:

– обеспечивает временную блокировку скомпрометированного Ключа ЭП (УНЭП, УКЭП) УЛ Клиента в Системе ДБО. Временная блокировка Ключа PayControl/ Устройства подтверждения УЛ Клиента не осуществляется. Удаление Ключа PayControl/ Устройства подтверждения УЛ Клиента в Системе ДБО при обращении по телефону осуществляется после получения подтверждения по телефону подтверждения экстренной блокировки Ключей ЭП;

– обеспечивает совершение телефонного звонка Клиенту на номер телефона подтверждения экстренной блокировки Ключей ЭП. Информация о номере телефона подтверждения экстренной блокировки Ключей ЭП указывается Клиентом в Заявлении в целях получения подтверждения факта Компрометации/ подозрения на Компрометацию.

- Банк в случае, если по факту телефонного звонка Клиенту подтверждение необходимости блокировки Ключа ЭП/ удаления Ключа PayControl/ Устройства подтверждения УЛ не получено:

– снимает временную блокировку Ключа ЭП (УНЭП, УКЭП), установленную по факту входящего телефонного звонка заявителя, не удаляет Ключ PayControl/ Устройство подтверждения. Иные действия в Системе ДБО в случае необходимости Банк совершает на основании предоставленного Клиентом Заявления о компрометации.

В случае не предоставления Клиентом в Банк номера телефона подтверждения экстренной блокировки Ключей ЭП, блокировка скомпрометированного Ключа ЭП, удаление Ключа PayControl/ Устройства подтверждения УЛ Клиента на основании входящего телефонного звонка Клиента не осуществляется.

– По факту получения от Клиента информации о Компрометации или в случае выявления Банком факта Компрометации/ любых подозрений на Компрометацию (при наличии у Банка информации о событиях, относящихся к Компрометации), Банк незамедлительно блокирует скомпрометированный Ключ ЭП, удаляет Ключ PayControl/ Устройство подтверждения УЛ Клиента в Системе ДБО, прекращает приём и исполнение ЭД, подписанных скомпрометированным Ключом ЭП/ Ключом PayControl.

– В целях получения нового Пароля, Ключевого носителя (USB-Токен), Устройства подтверждения Клиент либо запрашивает их в Заявлении о компрометации в момент уведомления Банка о наступлении случая Компрометации, либо подаёт в Банк Заявление об изменении данных в порядке, определённом подп. **Ошибка! Источник ссылки не найден.** Правил.

– Генерацию новых Ключей ЭП/ Ключей PayControl Клиент осуществляет в соответствии с разделом **Ошибка! Источник ссылки не найден.** Правил.

Не вносить исправления, изменения или дополнения в специализированное программное обеспечение и техническую документацию, предоставленные Банком по Договору ДБО, не передавать их третьим лицам, а также не передавать третьим лицам Ключевые носители, Устройства подтверждения, сведения по форматам ЭД и технологии их обработки Клиентом и Банком, а также прочие сведения, относящиеся к Договору ДБО.