

Обязательства Участника по выполнению правил безопасной работы при использовании системы дистанционного банковского обслуживания

Участник подтверждает, что для обеспечения безопасной работы в Системе следующие организационные меры будут соблюдаться всеми Уполномоченными лицами Участника.

1. Выполнение следующих правил выбора пароля доступа к ключам ЭП:

- Пароль выбирается самостоятельно владельцем Ключа ЭП;
- Если пароль записан на бумаге, то хранится в месте, недоступном для третьих лиц;
- Пароль содержит не менее 6 различных символов;
- Пароль обязательно меняется, если он стал известен постороннему лицу;
- В качестве пароля не используются:
 - последовательности, состоящие из одних цифр (в том числе даты, номера телефонов, номер автомобиля и т.п.);
 - последовательности повторяющихся букв или цифр;
 - идущие подряд в раскладке клавиатуры или в алфавите символы;
 - имена и фамилии;
 - ИНН или другие реквизиты Участника.

2. При эксплуатации USB-токена необходимо соблюдать следующие меры предосторожности:

- не разбирать;
- не допускать механических воздействий (падений, сотрясений, вибраций);
- не допускать воздействий влаги и агрессивных сред;
- не допускать воздействий высоких и низких температур;
- не допускать воздействия сильных электромагнитных, радиационных полей, высокого напряжения и статического электричества;
- не прилагать излишних усилий при подсоединении USB-токена к порту компьютера;
- запрещается:
 - оставлять USB-токен без контроля, в том числе при покидании пользователем своего рабочего места;
 - передавать USB-токен третьим лицам;
 - сообщать третьим лицам пароль от ключей электронной подписи. В случае утери (хищения) или повреждения, а также некорректной работы USB-токена требуется немедленно обратиться в Банк.
- Пароль от USB-токена должен иметь длину минимум 8 символов. Пароль должен содержать в себе строчные и прописные буквы, цифры и специальные знаки. Безопасный пароль не должен состоять из последовательно расположенных на клавиатуре символов.
- USB-токены и пароли доступа к ним хранятся в недоступном для окружающих месте отдельно друг от друга;
- По завершении работы в Системе или в перерыве в работе (включая кратковременный) USB-токен отсоединяется от компьютера;
- USB-токен используется только для подписания электронных документов;
- USB-токен не передается третьим лицам даже на короткое время;

- В случае смены Уполномоченного лица Участника, осуществляющего подпись электронных документов с использованием данного USB-токена, утери USB-токена, а также о любом подозрении на компрометацию ключа ЭП незамедлительно сообщается в Банк для блокировки Ключа проверки ЭП с последующим направлением в Банк письменного уведомления.
- 3. Ограничение доступа к рабочим местам, с которых осуществляется работа сотрудников Участника в Системе (далее «Рабочие места Системы»):**
- Право доступа предоставляется только лицам, непосредственно осуществляющим работу в Системе;
 - Рабочие места Системы не оставляются без контроля: при кратковременном отсутствии сотрудника Участника сохраняются все открытые на редактирование документы, средствами операционной системы блокируется рабочее место.
- 4. Исключение несанкционированного изменения программного обеспечения на рабочих местах Системы:**
- Используется только лицензионное программное обеспечение;
 - Устанавливаются все обновления системы безопасности, рекомендуемые производителем операционной системы, установленной на компьютере;
 - Отключаются учетные записи, позволяющие анонимный (гостевой) вход в операционную систему, установленную на компьютер;
 - Блокируется возможность автоматической регистрации пользователя в операционной системе без ввода им паролей или парольных фраз, предъявления аппаратных устройств (электронных ключей или смарт-карт), средств достоверного опознавания биометрических характеристик пользователя, или использования иных аутентификационных механизмов;
 - Отключаются режимы отображения окна всех зарегистрированных в операционной системе пользователей и быстрого переключения пользователей (ОС Windows XP или более новая версия);
 - Для всех учетных записей в операционной системе используются пароли, удовлетворяющие требованиям пункта 1 настоящих Обязательств;
 - Для защиты от несанкционированного доступа из внешней или локальной сети используется и оперативно обновляется специализированное ПО для защиты информации — антивирусное ПО с регулярно обновляемыми базами, персональные межсетевые экраны, средства защиты от несанкционированного доступа.
- 5. Соблюдение правил безопасной работы в сети Интернет на Рабочих местах Системы:**
- Предпринимать организационные и технические меры по противодействию несанкционированному доступу третьих лиц:
 - к клиентскому рабочему месту (персональному компьютеру, ноутбуку, смартфону и т.п.), с помощью которого осуществляется взаимодействие с Системой;
 - к конфиденциальной информации Системы (Пароль, Коды авторизации);
 - к Средствам авторизации.
 - На клиентском рабочем месте (персональном компьютере, ноутбуке, смартфоне и т.п.), с помощью которого осуществляется взаимодействие с Системой:
 - ограничить использование административных полномочий;
 - использовать антивирусное программное обеспечение, настроенное на автоматическое обновление антивирусных баз и программных модулей;

- своевременно (в наилучшем случае – автоматически) обновлять компоненты операционной системы и используемого браузера, как минимум в части исправления обнаруженных уязвимостей;
- использовать персональные межсетевые экраны (брандмауэры), в том числе возможно встроенные в операционную систему;
- при наличии возможности физического доступа посторонних лиц к рабочему месту – использовать пароль для учетной записи операционной системы длиной не менее 6 символов и автоматическую блокировку экрана с паролем при бездействии в течение более 15 минут.
- Перед началом работы обязательно убедиться в том, что соединение установлено именно с сайтом Системы (<https://ibc.severgazbank.ru>), и в том, что соединение установлено именно в безопасном режиме, т.е. адресная строка в браузере начинается с символов « **https://** ».
- Не допускается открывать сайт Системы по ссылкам (особенно баннерным или полученным через почту);
- Не допускается отвечать на подозрительные письма с просьбой выслать ключ ЭП, пароль и другие конфиденциальные данные;
- Не допускается запускать на исполнение или сохранять в файловой системе компьютера подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях;
- На компьютере не производится установка программного обеспечения, полученного из ненадежных источников;
- Не рекомендуется посещать непроверенные сайты в сети Интернет, особенно те, которые распространяют пиратское программное обеспечение, музыкальные и видеофайлы, так как при входе на такие сайты можно заразить компьютер вредоносными программами;

6. Противодействие вредоносным программам при работе с Системой:

- При работе с Системой следует помнить, что ни один антивирус не гарантирует полную защиту от вредоносных программ, которые постоянно совершенствуются их авторами. Необходимо максимально серьезно относиться к поступающим из Банка предупреждениям о возможном заражении компьютера Участника вредоносной программой и следовать рекомендациям сотрудников Банка;
- Если Участник использует более одной ЭП для подписания электронных документов, то Ключи ЭП разных Уполномоченных лиц Участника рекомендуется хранить на разных USB-токенах и использовать на разных компьютерах. Это позволит существенно снизить риск негативных последствий в случае заражения вредоносной программой одного из компьютеров Участника;
- Использование дополнительных средств подтверждения платежей существенно снижает риск отправки платежного документа вредоносной программой. При использовании таких средств, например, одноразовых SMS-паролей, важно обращать внимание на присылаемую в SMS вместе с паролем проверочную информацию о подтверждаемом платеже. Это позволит избежать подмены платежных реквизитов вредоносной программой.