Приложение 9

к Договору банковского счета юридического лица/индивидуального предпринимателя/физического лица, занимающегося в установленном законодательством Российской Федерации частной практикой

в АКБ «ТЕНДЕР-БАНК» (АО)

**ТРЕБОВАНИЯ**

**по защите от вредоносного кода рабочего места Клиента,**

**предназначенного для установки системы ДБО**

В связи с участившимися случаями попыток проведения злоумышленниками мошеннических операций с использованием систем дистанционного банковского обслуживания (ДБО) по каналам сети Интернет, рекомендуем Вам обратить особое внимание на организационно-технические меры и правила обращения с ключевой информацией, используемой Вами при работе в системе электронного банкинга.

В этой связи, Банк реализует комплекс мероприятий организационного и технического характера, направленных на обеспечение защиты информации. Соблюдение правил информационной безопасности (ИБ) призвано обеспечить защищенность интересов кредитной организации и её клиентов в условиях угроз в информационной сфере при оказании услуг ДБО.

Задачи ИБ сводятся к минимизации ущерба, а также к прогнозированию и предотвращению случайных или злонамеренных воздействий. Для обеспечения надлежащей степени защищенности необходимо использование комплексного подхода, когда вопросам ИБ уделяется достаточно внимания, как на стороне банка, так и на стороне клиента.

Поскольку основное количество схем хищений направлено на реализацию различных атак на процедуры и технологии расчетов с использованием электронных средств платежа, включая системы ДБО, то и основные мероприятия ориентированы на защиту этих средств.

**Для минимизации рисков при использовании дистанционного банковского обслуживании Банк рекомендует Клиентам:**

* Использовать в работе только лицензионные версии операционных систем и прикладного программного обеспечения;
* Применять и своевременно обновлять средства антивирусной защиты;
* Своевременно устанавливать обновления безопасности для используемого ПО;
* Определить последовательность необходимых действий, осуществляемых при возникновении внештатной ситуации или при подозрении на неё;
* Ключевой носитель с **рабочими ключами электронной подписи (ЭП)** нельзя передавать третьим лицам, оставлять без присмотра, хранить в доступном месте;
* Ключевой носитель должен использоваться только владельцем сертификата ключевой информации, либо лицом, уполномоченным на использование ЭП;
* На электронном носителе (дискета, флеш-карта, CD), на котором расположены ключи ЭП, не должно быть **другой информации**;
* Хранение закрытого ключа ЭП на жёстком диске **НЕДОПУСТИМО**;
* По истечении срока действия ключа ЭП, нео**бходимо провести** его плановую замену;
* Настоятельно не рекомендует**ся использо**вать компьютер, на котором установлена система ДБО для выполнения поиска в сети интернет, посещения развлекательных и прочих ресурсов, официальный владелец которых не известен или не вызывает доверия;
* Не желательна работа с системой ДБО с гостевых рабочих мест (интернет-кафе и т.д.);
* К компьютеру должен быть исключен доступ (физический и/или удаленный) лиц, не имеющих полномочий для работы в системе ДБО;
* В случае передачи (списания) 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 Вашей организации, в том числе следы работы в системе ДБО;
* Настоятельно рекомендуем, при работе с системой ДБО использовать USB-Токены и «Смарт-Карты». Защищенное хранение и неизвлекаемость секретного ключа ЭП при использовании USB-токена делает невозможным хищение секретных ключей ЭП, используемых при работе в системе;
* Сменный носитель с ключевой информацией должен быть установлен в считывающее устройство компьютера только на время проведения платежной операции и операций обмена с Банком. Размещение сменного носителя в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами;
* Регулярно меняйте пароль для работы в системе ДБО. Используйте сложные пароли, чтобы длина Вашего пароля была не менее 8 символов, и представлял собой сочетание заглавных и прописных букв, цифр и, если возможно, спецсимволов. Мы крайне не рекомендуем Вам использовать простые пароли (например, имена, фамилии, номера телефонов, года рождения и т.д.).

**Противодействие инсайдерам**

Наибольшими возможностями для нанесения ущерба при осуществлении дистанционного банковского обслуживания обладает собственный персонал (инсайдеры), а также ненадлежащим образом защищенная (с точки зрения ИБ) территория размещения автоматизированных рабочих мест (АРМ) ДБО Клиента. Для обеспечения защиты от атак с участием инсайдеров Банк рекомендует предусмотреть:

* разработку и внедрение строгой политики ролей и прав сотрудников, разграничение доступа к информационным ресурсам;
* использование сетевых брандмауэров (FireWall) для фильтрации и разграничения доступа сотрудников как к внешним, так и к внутренним ресурсам;
* организацию физического доступа в помещения, в которых функционирует система ДБО.

**При смене, увольнении лица, имеющего, даже потенциально, доступ к ключевому носителю (например, системного администратора), необходимо незамедлительно:**

* Сменить пароль доступа в систему ДБО Банка;
* Произвести перегенерацию ключей ЭП при содействии сотрудников Банка.

**Просим вас незамедлительно обращаться в банк при возникновении следующих ситуаций:**

* На компьютере, используемом для работы в системе ДБО, обнаружено вредоносное ПО (вирусы, «трояны» и т.д.);
* Обнаружены факты проникновения в систему посторонних лиц;
* В выписке обнаружены несанкционированные Вами расходные операции;
* У Вас не работает система ДБО по неизвестным причинам;
* Компьютер, используемый для обмена с Банком, по непонятным причинам, перестал функционировать;
* Частые зависания и повторяющиеся ошибки компьютера с установленной системой ДБО;
* Также, согласно статистике противоправных действий в системах ДБО, самым опасным временем работы в системе ДБО является пятница и предпраздничные дни, после 15-00. Так как, некоторые банки работают по сокращенному рабочему дню, остановить несанкционированный платеж в преддверии выходных очень проблематично;
* Обращаем Ваше внимание, что **своевременное** обращение в Банк позволит принять оперативные меры по предотвращению мошенничества. Сотрудники Отдела автоматизации готовы оказать помощь по вопросам соблюдения требований безопасности при работе в сети Интернет и использования систем ДБО.