## Рекомендации по мерам безопасности и защите информации от воздействия вредоносного кода при использовании системы дистанционного банковского обслуживания «BS-Client».

**1. Рекомендации по защите информации от воздействия вредоносного кода.**

В рамках обеспечения защиты информации от воздействия вредоносного кода пользователям системы дистанционного банковского обслуживания рекомендуется:

– постоянно использовать средства антивирусной защиты (САЗ) на компьютерах, предназначенных для работы в системе дистанционного банковского обслуживания;

– установить настройки, обеспечивающие запуск САЗ в автоматическом режиме, в процессе загрузки операционной системы, а также постоянное функционирование в фоновом режиме в процессе работы;

– регулярно проверять все дискового пространства и оперативную память компьютеров, предназначенных для работы в системе дистанционного банковского обслуживания, на наличие вредоносных программ;

– ежедневно автоматически обновлять установленные САЗ и антивирусные сигнатурные базы;

– при работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, и/или переходить по содержащимся в таких письмах гиперссылкам;

– не производить установку каких-либо программ, загруженных из сети Интернет, кроме лицензионного программного обеспечения по ссылке, полученной от производителя;

– не использовать программы онлайнового общения на компьютере, предназначенном для работы в системе дистанционного банковского обслуживания;

– исключить возможность установки вредоносных программ (вирусов) посторонними лицами (гостями, посетителями) на компьютеры, предназначенные для работы в Системе;

– организовать работу пользователей от имени учетных записей, не имеющих права администраторов в операционной системе компьютера, предназначенного для работы в системе дистанционного банковского обслуживания;

– при подозрениях на наличие вредоносных программ (вирусов) на компьютере, предназначенном для работы в системе дистанционного банковского обслуживания, полностью воздержаться от использования системы дистанционного банковского обслуживания и проведения платежей до исправления ситуации.

**2. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет.**

Пользователям системы дистанционного банковского обслуживания рекомендуется соблюдать меры предосторожности при использовании сети Интернет для проведения расчетов с использованием системы дистанционного банковского обслуживания:

- в случае обнаружения в сети Интернет ложного веб-сайта АО «Тойота Банк», отличного от www.toyota.ru/toyota-fs/corp.tmex, а также, в случаях, если с вами пытаются связаться по электронной почте или иным способом лица, с требованиями о предоставлении персональных идентификаторов доступа к системе дистанционного банковского обслуживания, необходимо немедленно сообщить об этом в отдел расчетов АО «Тойота Банк» по телефону: **+7 (495) 644-10-70 или на электронный адрес settlements@toyota-fs.com.** Размещение информационных материалов АО «Тойота Банк» в сети Интернет осуществляется только по адресу – www.toyota.ru/toyota-fs/corp.tmex. АО «Тойота Банк» не использует WEB-сайт www.toyota.ru/toyota-fs/corp.tmex для осуществления расчетных операций в системе дистанционного банковского обслуживания.

**3. Рекомендации по снижению рисков получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не**

**обладающими правом распоряжения этими денежными средствами.**

Пользователям системы дистанционного банковского обслуживания рекомендуется соблюдать организационные меры по обеспечению информационной безопасности:

- вести учет ключевых носителей, используемых в системе дистанционного банковского обслуживания;
- хранить ключевые носители для системы дистанционного банковского обслуживания (флеш-накопитель USB) в опечатанном (опломбированном) сейфе (контейнере), доступ к которому должен быть строго ограничен и предоставляться только уполномоченным лицам. Целостность печати (пломбы) следует контролировать ежедневно, в начале рабочего дня уполномоченным лицом. После завершения работы ключевой носитель помещается в сейф (контейнер) и заново опечатывается (пломбируется) уполномоченным лицом;
- использовать компьютер, предназначенный для работы в системе дистанционного банковского обслуживания, для выполнения задач связанных с осуществлением деятельности по переводу денежных средств;
- в случае временного перерыва в работе (совещание, обед и т.д.) на компьютере, предназначенном для работы в системе дистанционного банковского обслуживания, необходимо завершить работу в системе дистанционного банковского обслуживания, убрать в сейф (контейнер) ключевой носитель, выключить компьютер или заблокировать его клавиатуру и экран путем нажатия комбинации клавиш: «WIN» и «L»;
- не записывать пароли на бумажных листках (или в текстовых файлах на компьютере), оставлять их в легкодоступных местах (на рабочем столе), передавать неуполномоченным лицам. В случае необходимости, хранение паролей следует осуществлять в сейфе, в опечатанном конверте;
- в случае любых кадровых перестановок лиц, имевших доступ к компьютеру, системе дистанционного банковского обслуживания, ключевым носителям, при подозрении в несанкционированном доступе (локально или по сети) неуполномоченных лиц к компьютеру, системе дистанционного банковского обслуживания, ключевым носителям, паролям или других случаях нарушения информационной безопасности Клиенту следует сообщать об этом в АО «Тойота Банк».