**Приложение № 1**
к Условиям дистанционного обслуживания
клиентов с использованием Системы «iBank 2»

# ПРАВИЛА
# использования Системы «iBank 2»

В настоящих Правилах понятия Рабочее место и Вредоносный код используются в соответствии с терминологией Условий дистанционного обслуживания клиентов по системе «iBank 2».

Во исполнение пункта 3 статьи 9 Федерального закона «О национальной платежной системе» БАНК настоящим информирует КЛИЕНТА о следующем:

1. Использование клиентской части Системы «iBank 2» (далее – Система) допускается из любых мест и любыми возможными способами с учетом указанных ниже ограничений.

2. Использование Системы не рекомендуется в следующих случаях (включая, но не ограничиваясь):

2.1. КЛИЕНТОМ не выполнены Требования по защите от Вредоносного кода; Требования по обеспечению безопасности при работе с системой дистанционного банковского обслуживания «iBank2».

2.2. На Рабочем месте КЛИЕНТА не установлены полученные из доверенных источников сертифицированные ФСБ средства криптографической защиты информации (СКЗИ);

2.3. КЛИЕНТ не обеспечил надежное хранение и защиту от компрометации средств, использующихся для дистанционного распоряжения счетом КЛИЕНТА (Средства подтверждения

2.4. КЛИЕНТ не ознакомился с правилами работы с Системой и правилами работы с СКЗИ;

2.5. КЛИЕНТ не обеспечил периодическую (но не реже 1 раза в год) смену паролей для доступа к своему Рабочему месту или к ключу ЭП;

2.6. КЛИЕНТОМ был обнаружен отказ специализированного ПО, используемого для защиты информации, или отказ клиентской части Системы;

2.7. КЛИЕНТОМ не обеспечен запрет использования на Рабочем месте средств удаленного управления (R-Admin, TeamViewer и аналоги), администрирования и модификации ОС и её настроек (службы терминалов, удаленных рабочих столов и аналоги);

2.8. У КЛИЕНТА не настроены минимум два канала оповещения о совершении операций.

3.КЛИЕНТ уведомлен, что при использовании Системы он несет повышенные риски, связанные с несанкционированным списанием средств КЛИЕНТА неуполномоченными лицами, в том числе и с использованием Вредоносного кода. Начиная работать с Системой, КЛИЕНТ подтверждает, что он полностью принимает на себя указанные риски.

4. КЛИЕНТ несет полную ответственность за действия, совершенные третьими лицами, в случае передачи КЛИЕНТОМ Средств подтверждения указанным лицам и/или в случае создания КЛИЕНТОМ условий для несанкционированного использования третьими лицами Средств подтверждения. КЛИЕНТ также несет полную ответственность за ущерб, причиненный БАНКУ, указанными действиями или бездействием.

5. КЛИЕНТ согласен с использованием логов (журналов) Системы и журналов модуля Системы по детектированию вредоносного программного обеспечения в качестве доказательства при разбирательстве по факту нарушений настоящих Правил и требований по защите от Вредоносного кода.

6. КЛИЕНТ уведомлен, что при использовании одного Аппаратного средства усиленной ЭП для хранения Ключей ЭП нескольких сотрудников он несет повышенные риски, связанные с несанкционированным списанием средств КЛИЕНТА неуполномоченными лицами, в том числе и с использованием Вредоносного кода. БАНК рекомендует КЛИЕНТУ использовать Аппаратное средство усиленной ЭП для хранения одного Ключа ЭП одного сотрудника. Начиная работать с Системой, КЛИЕНТ подтверждает, что он полностью принимает на себя указанные риски.

7. КЛИЕНТ уведомлен и согласен, что ключи ЭП различных сотрудников КЛИЕНТА, имеющих право подписи платежных документов должны создаваться и храниться на отдельных Аппаратных средствах усиленной ЭП.