

Памятка об ограничениях способов и мест использования, случаях повышенного риска использования Системы дистанционного банковского обслуживания

В целях исполнения требований п. 3 ст. 9 Федерального закона от 27.06.2011 №161-ФЗ «О национальной платежной системе» КМ «Профильный Банк» (АО) (далее – Банк) информирует Клиента – юридическое лицо, индивидуального предпринимателя, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, (далее – Клиент) о следующем.

1. Использование клиентской части Системы дистанционного банковского обслуживания (далее – Система ДБО) допускается из любых мест и любыми возможными способами с учетом указанных ниже ограничений.

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

2.1. Клиентом не соблюдаются Рекомендации для Клиентов по информационной безопасности (далее – Рекомендации по информационной безопасности) при работе с Системой ДБО. Рекомендации по информационной безопасности доводятся до Клиентов путем размещения документа на официальном сайте Банка в информационно – телекоммуникационной сети «Интернет» по адресу: <https://profilbank.ru/>.

2.2. На рабочем месте Клиента не установлены полученные из доверенных источников сертифицированные Федеральной службой безопасности средства криптографической защиты информации (СКЗИ).

2.3. Клиент не обеспечил надежное хранение и защиту от компрометации USB-токен, содержащий ключ электронной подписи (далее – ключ ЭП), номер(-а) мобильного(-ых) телефона, использующихся для дистанционного распоряжения счетом Клиента.

2.4. Клиент не ознакомился с условиями дистанционного банковского обслуживания клиентов - юридических лиц (в том числе кредитных организаций), индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в КМ «Профильный Банк» (АО) и Рекомендациями по информационной безопасности.

2.5. На рабочем месте Клиента установлено программное обеспечение (ПО), полученное не из доверенных источников или нелицензионное программное обеспечение.

2.6. Клиент не обеспечил периодическую (но не реже 1 раза в год) смену паролей для доступа к своему рабочему месту или к ключу ЭП.

2.7. Клиентом был обнаружен отказ специализированного ПО, используемого для защиты информации, или отказ клиентской части Системы ДБО.

2.8. Клиентом не обеспечен запрет использования на рабочем месте средств удаленного управления (R-Admin, TeamViewer и аналоги), администрирования и модификации операционной системы и её настроек (службы терминалов, удаленных рабочих столов и аналоги).

2.9. Клиентом не обеспечена защита рабочего места от проникновения вредоносных программ и программ, позволяющих, пользуясь ошибками системного и прикладного ПО, повышать предоставленные привилегии.

2.10. Клиентом не обеспечено регулярное обновление антивирусных программ, обновление прикладного ПО, установка пакетов обновления безопасности операционной системы.

3. Клиент уведомлен, что при использовании Системы ДБО он несет повышенные риски, связанные с несанкционированным списанием средств Клиента неуполномоченными лицами. Начиная работать с Системой ДБО, Клиент подтверждает, что он полностью принимает на себя все указанные риски.