РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ
при использовании системы дистанционного банковского обслуживания

Придерживайтесь следующих правил:

— Подключите e-mail или SMS/push-уведомления об отправке платежей и при обнаружении подозрительных операций незамедлительно обращайтесь в банк!

— Используйте встроенные средства блокировки и разблокировки мобильного телефона (логин/пароль для входа в ОС, логин/PIN-код/отпечаток пальца).

Важно понимать, что:

— Банк не имеет доступа к паролям Клиентов для входа в систему.

— Вся ответственность за конфиденциальность паролей полностью лежит на Клиенте как на единственном владельце.

— Банк не рассылает по электронной почте и не озвучивает по телефону пароли Клиента.

— Банк никогда не запрашивает по электронной почте и по телефону пароли, номер банковской карты Клиента и ПИН-коды.

— Если Клиент сомневается в конфиденциальности своих паролей или есть подозрение в их компрометации, Клиент должен произвести смену своих паролей с использованием мобильного или Интернет-банка.

— В случае обнаружения подозрительных веб-сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением веб-сайтов Бланк банка, просьба сообщить об этом в Банк любым доступным способом.

— Необходимо регулярно проверять состояние счетов и движение документов по выпискам.

— Нельзя вводить конфиденциальные данные, если окно для ввода отличается от стандартных окон Системы «Клиент-Банк» (другие надписи, шрифт и тому подобное) или отображается не так, как всегда (нарушен порядок работы в системе). О появлении подобных сайтов немедленно сообщите в Банк любым доступным способом.

— После окончания работы в системе ДБО необходимо всегда использовать пункт меню «Выход».

Соблюдайте общие правила безопасности для защиты данных, хранящихся на компьютерах

— Используйте только доверенные компьютеры и смартфоны с лицензионными программами и установленным антивирусом. Регулярно проверяйте компьютер и смартфон на вирусы, производите обновления программного обеспечения и антивирусных баз.

— При работе с электронной почтой не открывайте письма, полученные от неизвестных отправителей, и вложения к ним, не переходите по ссылкам из таких писем.

— Не используйте права администратора без крайней необходимости. В повседневной практике входите в систему как пользователь без прав администратора.

— При работе в сети Интернет не соглашайтесь на установку дополнительных программ.

— По возможности используйте выделенный компьютер и смартфон только для работы с мобильным и Интернет-банком.

— Не сохраняйте логин и пароль на общедоступных компьютерах/терминалах и не записывайте их в электронные файлы.

— Храните в тайне номер банковской карты, срок её действия и CVV-код.

Незамедлительно надо обратиться в Банк, если:

— Возникло подозрение, что пароль был скомпрометирован.

— Была обнаружена иная подозрительная активность в системе ДБО.

BLANC