Рекомендации по повышению уровня безопасности платежей в системе «Клиент-Банк»:

1. Для работы с системой «Клиент-Банк» рекомендуется использовать отдельный компьютер, доступ к которому имеют только лица, осуществляющие платежи в системе «Клиент-Банк». При этом необходимо соблюдать правила информационной безопасности, регламент доступа к компьютерам для работы в системе «Клиент-Банк», регламент работы с секретными ключами ЭЦП.
2. На компьютере, с которого осуществляется работа в системе «Клиент-Банк», необходимо использовать только лицензионное системное и прикладное ПО, оперативно его обновлять; использовать и оперативно обновлять персональный межсетевой экран (firewall), антивирусное ПО, средства обнаружения вредоносных программ.
3. При использовании двух секретных ключей ЭЦП (ключ ЭЦП директора с правом первой подписи, и ключ ЭЦП главного бухгалтера с правом второй подписи) желательно осуществлять работу с системой «Клиент-Банк» на двух отдельных компьютерах с хранением секретных ключей ЭЦП на двух отдельных USB-токенах.
4. В качестве хранилища ключей ЭЦП рекомендуется использовать USB-токен. Использование USB-токена позволяет существенно снизить вероятность хищения ключей ЭЦП злоумышленниками.
5. Наиболее эффективной мерой, позволяющей оперативно реагировать на возможные мошеннические действия третьих лиц, и при этом отслеживать платежи и операции, проводимые по счёту, является использование информационной услуги SMS-Банкинга.

   В качестве дополнительной меры безопасности возможно использование услуги дополнительного подтверждения отправки всех документов, либо документов, превышающих определенную сумму, с помощью одноразовых паролей, отправляемых по SMS.

   За более подробной информацией о данной услуге обратитесь к специалисту Банка.