Лайтбанк
Москва, ул. Новая Басманная, 22/2
Тел. (495) 644-33-37
E-mail: support@lightbank.ru
www.lightbank.ru

ПАМЯТКА
о мерах по защите информации при использовании системы интернет-банк.

Уважаемый клиент, для обеспечения достаточного уровня защиты информации при работе с системой “Интернет-банк” настоятельно рекомендуем соблюдать следующие меры компьютерной безопасности:

1. Использовать лицензионное ПО (операционные системы, офисные пакеты и пр.), обеспечить своевременное автоматическое обновление системного и прикладного ПО (нереже одного раза в неделю);
2. Применять на рабочем месте современные лицензионные средства антивирусной защиты (Dr.Web, Антивирус Касперского и др.), обеспечить возможность своевременного автоматического обновления антивирусных баз, а также регулярно производить полное сканирование компьютера (не реже одного раза в неделю);
3. Включить систему защиты брандмауэр Windows или установить персональный межсетевой экран (firewall);
4. Изолировать доступ к компьютеру из любых компьютерных сетей (ЛВС организации, Интернет и др.), а также запретить доступ любых интернет-сайтов за исключением доступа к системе “Интернет-банк” ООО КБ «ЛайтБанк» **(URL адрес: https://ibank.lightbank.ru/ IP адрес: 213.79.93.86)**, а также доступа к серверам обновлений операционной системы и антивирусных баз.
5. Работу на компьютере осуществлять только с правами ПОЛЬЗОВАТЕЛЯ;
6. Исключить использование любого программного обеспечения развлекательного и социального характера и др., за исключением необходимого для работы;
7. Подсоединять носитель ключевой информации к компьютеру **только** в момент начала работы с интернет-банком, и **обязательно** извлекать его из компьютера сразу после окончания работы;
8. При обслуживании компьютера ИТ-сотрудниками – обеспечивать контроль за выполняемыми ими действиями;
9. Не передавать ключи ЭЦП ИТ-сотрудникам для проверки работы системы "Интернет-банк", проверки настроек взаимодействия с банком и т.п. При необходимости таких проверок **только лично владелец ключа ЭЦП должен подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа системы, и лично ввести пароль.**
10. При увольнении ответственного сотрудника, имевшего доступ к секретному (закрытому) ключу ЭЦП, обязательно позвонить в банк и заблокировать ключ ЭЦП.
11. При увольнении сотрудника, имевшего технический доступ к секретному (закрытому) ключу ЭЦП, обязательно позвонить в банк и заблокировать ключ ЭЦП.
12. При увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с системой "Интернет-банк",произвести проверку антивирусными средствами для обеспечения отсутствия редоносных программ на компьютерах.
13. При возникновении подозрений на компрометацию (копирование) секретных (закрытых) ключей ЭЦП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно позвонить в банк и заблокировать ключи ЭЦП.
14. Регулярно проводить контроль сумм и получателей платежных документов в информационном окне системы интернет-банка, а также контролировать количество и сумму отправленных документов;
15. Регулярно контролировать состояние своих счетов и незамедлительно информировать ООО КБ «ЛайтБанк» обо всех подозрительных или несанкционированных операциях.
16. В случае выхода из строя ПК, либо некорректной работы системы интернет-банка, или признаков наличия вредоносного ПО, а также нестандартного поведения ПК, **необходимо незамедлительно прекратить работу на ПК, вынуть носитель ЭЦП, отключить ПК от всех видов сетей, включая локальную корпоративную сеть, срочно запросить в ООО КБ «ЛайтБанк» выписку по счету**, и сообщить о данном случае Вашему Руководителю / ИТ-специалисту, а также позвонить в службу технической поддержки ООО КБ «ЛайтБанк» для получения рекомендаций.
17. При обнаружении несанкционированных платежных операций информировать руководство, обязательно позвонить в Банк и заблокировать ключи ЭЦП и написать официальное письмо, а также обратиться с соответствующим заявлением в правоохранительные органы.

Работоспособность поврежденного ПК не восстанавливать до проведения технической экспертизы. Работу с системой интернет-банка проводить только на новом ПК после смены всех своих ключей ЭЦП.

Рекомендации по обеспечению безопасности с помощью дополнительных услуг банка:

- Подключить услугу «IP-фильтрация» (информация, передаваемая в Банк по системе интернет-банк, будет обработана только в случае совпадения IP-адреса передающего компьютера, с IP-адресом Клиента, хранящимся в базе данных Банка)