Далена·Банк

111024, Москва, ш. Энтузиастов, 17, стр.1
Телефон/факс: +7 (495) 673-10-10
www.dalenabank.ru, dln@dalenabank.ru

Приложение № 7
к Договору дистанционного банковского обслуживания
по Системе «Клиент-Банк» («iBank 2»)

ПАМЯТКА КЛИЕНТА

о возможных угрозах хищения денежных средств с использованием Системы «Клиент-Банк» («iBank 2») и способах защиты

Сегодня хакерские атаки на счета предприятий, мошенничество с использованием вирусных программ – это не миф, а реальная угроза для бизнеса. При этом кража средств зачастую происходит из-за недостаточного внимания и конфиденциальности данных со стороны самих компаний.

Хищение средств с расчетных счетов возможно при получении злоумышленниками доступа к Секретным ключам ЭП и паролям. Для исключения несанкционированного доступа в Систему «Клиент-Банк» ООО МИБ «ДАЛЕНА» проводит комплекс мероприятий для повышения Вашей информационной и финансовой безопасности.

Убедительно просим Вас ознакомиться с «Памяткой о возможных угрозах хищения денежных средств с использованием Системы «Клиент-Банк» («iBank 2») и способах защиты» и настоятельно рекомендуем придерживаться правил, указанных в ней. Они позволят защитить Ваши счета и информацию от взлома.

Обращаем Ваше внимание на то, что все платежи в Системе «Клиент-Банк» («iBank 2») обязательно подтверждаются одноразовыми паролями (система многофакторной аутентификации).

- Для хранения файлов с секретными ключами ЭП используйте внешние носители. Наилучшими носителями являются **USB-токен «Рутокен ЭЦП 2.0»** или функционально полностью аналогичная ему **Смарт-карта «ЭЦП 2.0 Flash»**, подключаемая через CCID-совместимый картридер. Так как формирование ЭП ЭД происходит внутри токена, то ключ ЭП никогда не извлекается из токена. Технически подтверждено, что ни разработчик, ни владелец, ни злоумышленник не могут никаким способом считать ключ ЭП из токена.
- По завершении работы всегда вынимайте внешние носители из компьютера. Никогда не передавайте их третьим лицам и храните отдельно, например: в личном сейфе.
- Для обеспечения дополнительной защиты от несанкционированного доступа к **USB-токену «Рутокен ЭЦП 2.0»** установите PIN-код. PIN-код должен состоять не менее чем из 6 символов и может содержать любую комбинацию из букв, цифр и знаков препинания. При неправильном вводе PIN-кода более 15 раз подряд доступ к USB-токену блокируется. То есть у лица, незаконно завладевшего токеном, при сложном пароле нет возможности его подобрать при 15-ти попытках.
- Никогда не передавайте третьим лицам одноразовые пароли для подтверждения платежей, приходящие Вам из Банка в виде SMS-сообщений.

111024, Москва, ш. Энтузиастов, 17, стр.1
Телефон/факс: +7 (495) 673-10-10
www.dalenabank.ru, dln@dalenabank.ru

- Используйте **IP-фильтрацию -** дополнительный сервис, запрещающий пользование ключами ЭП на компьютерах вне Вашего офиса. В этом случае информация от Вас будет обработана, только если IP-адрес передающего компьютера совпадет с адресом, указанным в базе данных Банка.
- **Используйте все возможности SMS-Банкинга**. Выбирайте максимальный набор услуг: сообщения о входе в Систему и о проведении платежей. Этим Вы сможете предотвратить сомнительные операции, оперативно связавшись с Банком.
- **Не храните** на носителях с ключами ЭП какую-либо **другую информацию.**
- **Не ставьте на компьютеры «пустые» или простые пароли**, например, 123456, qwerty – и периодически меняйте их. Рекомендуемая частота смены паролей -1 раз в месяц.
- **Используйте разные пароли для разных систем (вход в windows, вход в Сисиему «Клиент-Банк» (iBank 2), электронная почта).**
- **При вводе пароля исключите возможность доступа других лиц к просмотру пароля.**
- **Рекомендуется соблюдать следующие требования при создании пароля:**
  использовать числа (0-9);
  использовать Заглавные буквы
  использовать строчные буквы
  использовать специальные символы (@,#,$,%и т.д.).
- **Не передавайте ключи ЭП ИТ-сотрудникам для проверки работы** Системы и настроек взаимодействия с Банком. Если такая проверка необходима, владелец ключа ЭП должен лично подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа «iBank 2», и ввести пароль, исключая умышленное наблюдение посторонними лицами.
- **Не передавайте ключи ЭП замещающим сотрудникам** (заместителям, временно исполняющим обязанности). Для них необходимо получить персональные ЭП и внести их в банковскую карточку.
- **При увольнении сотрудника**, имевшего доступ к секретному ключу ЭП, **обязательно заблокируйте его ключ** ЭП;
- **При увольнении ИТ-специалиста**, обслуживавшего компьютеры, подключенные к Системе «Клиент-Банк» («iBank 2»), обязательно **проверьте их на отсутствие вредоносных программ.**
- **При продолжительной работе в Системе «Клиент-Банк» («iBank 2»)**, отключите и **извлеките из компьютера носители с ключами** ЭП, если они не используются. Носители с ключами должны находиться в компьютере только в момент подписания документов и извлекаться сразу после подписания документов.
- **Выделите отдельный компьютер для работы с Системой «Клиент-Банк» («iBank 2»)** и не выполняйте на нем никакие другие задачи.

111024, Москва, ш. Энтузиастов, 17, стр.1
Телефон/факс: +7 (495) 673-10-10
www.dalenabank.ru, dln@dalenabank.ru

- **Ограничьте доступ к компьютерам**, используемым для работы с Системой «iBank 2» и исключите к ним доступ персонала, не работающего с Системой.
- **Исключите обслуживание компьютеров**, используемых для работы в **Системе «Клиент-Банк» («iBank 2»), нелояльными ИТ-сотрудниками.**
- При обслуживании компьютера ИТ-сотрудниками, **обязательно контролируйте ход выполняемых ими действий.**
- **На компьютерах**, подключенных к **Системе «Клиент-Банк» («iBank 2»)**, никогда **не посещайте Интернет-сайты сомнительного содержания, не устанавливайте нелицензионное программное обеспечение** и т. п. Наиболее безопасным будет полный запрет на все соединения (входящие и исходящие) с глобальной сетью Интернет, оставив доступ к необходимым ресурсам.
- **Используйте только лицензионное программное обеспечение** и обеспечьте его автоматическое обновление.
- **Применяйте только лицензионные средства антивирусной защиты**, обеспечив автоматическое обновление антивирусных баз и еженедельную полную антивирусную проверку.
- **Используйте специализированные средства безопасности**: персональные файрволы, антишпионское программное обеспечение.
- **Проверяйте на наличие вирусов все файлы** и программы, загружаемые из глобальной сети Интернет, полученные по электронной почте и на внешних носителях (дискеты, флеш-накопители, CD/DVD).
- **Осуществляйте полную антивирусную проверку после вспомогательных операций** на компьютере, подключенном к **Системе «Клиент-Банк» («iBank 2»)**. Например, после решения технических проблем, подключения к глобальной сети Интернет, установки или обновления бухгалтерских и информационно-правовых программ.
- **Не допускайте работу под учётной записью Windows, имеющей права администратора.** Необходимо использовать учётную запись с ограниченными правами в операционной системе Windows, установленной на компьютере.
- **Не используйте средства удалённого (дистанционного) доступа в личных целях.** Использовать средства удаленного (дистанционного) доступа разрешено только при взаимодействии с тех.поддержкой Банка и только под Вашим контролем.
- **При возникновении подозрений** на копирование секретных ключей ЭП или наличие в компьютере вредоносных программ – **обязательно заблокируйте ключи ЭП.**
- **Если Вы заметили проявление необычного поведения Системы** или изменения в интерфейсе программы – срочно **позвоните в Банк** и уточните причину. Если изменения не связаны с обновлением версии программного обеспечения, заблокируйте ключи **ЭП.**

111024, Москва, ш. Энтузиастов, 17, стр.1
Телефон/факс: +7 (495) 673-10-10
www.dalenabank.ru, dln@dalenabank.ru

Предполагаемая аудитория мошенников

Хищение средств с расчетных счетов при получении доступа к секретным ключам **ЭП** и паролям с целью направления в Банк платежных поручений, заверенных от Вашего лица предположительно могут осуществить:

- Ответственные сотрудники Вашей компании, ранее имевшие доступ к секретным ключам **ЭП**, например, уволенные директора, бухгалтеры и их заместители, бывшие совладельцы Компании.
- Штатные ИТ-сотрудники Вашей компании, имеющие или имевшие технический доступ к носителям (дискеты, флеш-носители) с секретными ключами **ЭП** и к компьютерам компании, подключенным к **Системе «Клиент-Банк» («iBank 2»).**
- Внештатные, приходящие по вызову ИТ-специалисты, обслуживающие компьютеры Вашей компании, осуществляющие профилактику и подключение к глобальной сети Интернет, установку и обновление бухгалтерских, информационно-правовых и других программ на компьютеры, подключенные к Клиент-Банку.
- Другие злоумышленники путем заражения через глобальную сеть Интернет Ваших компьютеров вредоносными программами и хищения секретных ключей **ЭП** и паролей.

Таким образом, в Банк могут поступать не вызывающие подозрений платежи, направленные злоумышленниками с использованием действующих секретных ключей **ЭП**, имеющие обычные реквизиты получателей и типовые назначения платежа.

ООО МИБ «ДАЛЕНА» напоминает Вам о том, что:

- Банк не имеет доступа к Вашим секретным ключам **ЭП** и не может от Вашего имени сформировать корректную **ЭП** под электронным платежным поручением.
- Банк никогда не осуществляет рассылку электронных писем с просьбой прислать Ваш секретный ключ **ЭП** или пароль;
- Банк не рассылает по электронной почте программы для установки на Ваши компьютеры. Если Вы получили подобное письмо от имени Банка, содержащее программу для установки или запрос на предоставление ключей **ЭП** /паролей, срочно сообщите об этом в Службу технической поддержки клиентов Банка.
- Вы являетесь единственным владельцем секретных ключей **ЭП** и ответственность за их конфиденциальность лежит на Вас.
- Если Вы сомневаетесь в конфиденциальности секретных ключей **ЭП** или подозреваете компрометацию (копирование) данных, срочно заблокируйте Ваши ключи **ЭП**.
- Изменение пароля доступа к секретному ключу **ЭП** не защищает Вас от использования

111024, Москва, ш. Энтузиастов, 17, стр.1
Телефон/факс: +7 (495) 673-10-10
www.dalenabank.ru, dln@dalenabank.ru

злоумышленниками ранее похищенного ключа. В этом случае необходимо заблокировать старый ключ и получить новый.