ПРИЛОЖЕНИЕ № 11
к Договору на обслуживание клиентов в Системе Интернет-Банк
(редакция 5.0)

ПАМЯТКА КЛИЕНТА
о возможных угрозах хищения денежных средств и рекомендации по обеспечению информационной безопасности при работе в Системе Интернет-Банк

Атаки злоумышленников на банковские счета предприятий и частных лиц, мошенничество с использованием вредоносного программного обеспечения (вирусы, трояны, программы-вымогатели, вирусы, черви и др.) представляют реальную угрозу для бизнеса. Несанкционированное списание (хищение) средств чаще всего происходит из-за незнания или несоблюдения уполномоченными сотрудниками компаний требований по обеспечению Вашей информационной безопасности при работе с Системой Интернет-Банк. В целях исключения несанкционированного доступа в Систему Интернет-Банк АО КБ «Соколовский» проводит комплекс мероприятий по повышению Вашей осведомленности в вопросах информационной и финансовой безопасности. Убедительно просим Вас ознакомиться с настоящей Памяткой и настоятельно рекомендуем придерживаться указанных в ней рекомендаций и правил. Это позволит защитить Ваши счета и конфиденциальную информацию от взлома и несанкционированного использования, а также предотвратит утерю денежных средств.

Основные меры безопасности при работе в Системе Интернет-Банк (далее-Система/Система Интернет-Банк):

- Вход в Систему осуществляется с использованием Вашего Сертификата ключа проверки электронной подписи, пароля доступа к ключу ЭП (PIN-кода), а также одноразового пароля (СМС-кода), направляемого на номер Вашего мобильного телефона.

  При получении от Банка SMS-сообщения с одноразовым паролем внимательно ознакомьтесь с информацией в сообщении: реквизиты операции в сообщении должны соответствовать той операции, которую Вы собираетесь совершить. Только удостоверившись, что информация в этом SMS-сообщении корректна, можно вводить пароль

  Если для входа в Систему Вам предлагается ввести любую другую персональную информацию или дополнительные данные (Кодовое слово, персональные данные (номер паспорта, дату и место рождения, финансовую информацию или другие данные), это указывает на мошеннические действия! В таких случаях необходимо немедленно прекратить сеанс работы в Системе и срочно обратиться в Банк. **Помните! Вводя Одноразовый пароль, Вы даёте Банку распоряжение о проведении операции с указанными в SMS-сообщении реквизитами.**

  Ни при каких обстоятельствах не сообщайте пароли никому, включая сотрудников Банка.

- По завершении работы всегда отключайте и извлекайте из компьютера внешние носители с ключами ЭП. Никогда не передавайте их третьим лицам и храните отдельно, например, в личном сейфе.
- Работая с Персональным аппаратным криптопровайдером (ПАК), обязательно задавайте пароль (**PIN-код)** доступа достаточной сложности (Достаточной считается длина не менее 10 символов, среди которых Обязательно присутствуют строчные и прописные буквы, цифры, спецсимволы). Без его корректного ввода получить доступ к ключам ЭП невозможно.
- Используйте **IP-фильтрацию -** дополнительную возможность, запрещающую 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.
- **Не ставьте на компьютеры «пустые» или простые пароли**, например 123456, qwerty – и периодически меняйте их. Требования к сложности паролей для компьютера – аналогичны требованиям к паролям на ПАКах. Рекомендуемая частота смены паролей -1 раз в год.
- **Не передавайте ПАКи и ключевые носители 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 Интернет-Банк, и введите пароль, исключая умышленное наблюдение посторонними лицами.

- **Не передавайте ПАКи и ключевые носители замещающим сотрудникам** (заместителям, временно исполняющим обязанности). Для них необходимо получить персональные ЭП и внести их в банковскую карточку с образцами подписей и оттиска печати.
- **При увольнении сотрудника**, имевшего доступ к ключу ЭП, **обязательно заблокируйте его ключ** ЭП;
- **При увольнении ИТ-специалиста**, обслуживавшего компьютеры, подключенные к Системе Интернет-Банк, обязательно **проверьте их на отсутствие вредоносных программ**.
- **При продолжительной работе в Системе Интернет-Банк**, 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 Интернет-Банк** и не выполняйте на нем никакие другие задачи (по возможности).
- **Ограничьте доступ к компьютерам**, используемым для работы с Системой Интернет-Банк и исключите к ним доступ персонала, не работающего с Системой.
- При обслуживании компьютера ИТ-сотрудниками, **обязательно контролируйте ход выполняемых ими действий.**
- **На компьютерах**, подключенных к Системе, никогда **не посещайте Интернет-сайты сомнительного содержания, не устанавливайте нелицензионное программное обеспечение** и программное обеспечение, полученное из сети Интернет. Наиболее безопасным будет полный запрет на все соединения (входящие и исходящие) с сетью Интернет, кроме доступа к необходимым для деятельности ресурсам.
- **Используйте только лицензионное программное обеспечение** и обеспечьте его автоматическое обновление.
- **Применяйте только лицензионные средства антивирусной защиты**, обеспечив регулярное (не реже одного раза в день) автоматическое обновление антивирусных баз, резидентную защиту в реальном времени и еженедельную полную антивирусную проверку.
- **Используйте специализированные средства безопасности**: персональные межсетевые экраны, антишпионское программное обеспечение.
- **Проверяйте на наличие вирусов все файлы** и программы, загружаемые из Интернета, 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 Интернет-Банк. Например, после решения технических проблем, подключения к 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.
- **С особым вниманием используйте средства удалённого (дистанционного) доступа**, которые часто применяют IT-специалисты для удалённой поддержки. Заблокируйте возможность использования данных систем без непосредственного подтверждения со стороны пользователя АРМ, в остальное время закройте возможности удаленного доступа с помощью сетевого экрана (программного и/или аппаратного).
- Для защиты ключей ЭП от хищения вредоносными программами рекомендуется использовать аппаратное устройство (см. раздел Поддерживаемые аппаратные устройства «Краткого руководства пользователя системы дистанционного банковского обслуживания «iBank2» (Интернет-Банк)»).

- В случае отсутствия аппаратного устройства, сохраните файл-хранилище ключей на съемном носителе (USB-накопитель). Не допускается сохранять его в местах, где к нему может получить доступ кто-либо, кроме вас. **Съемный носитель с хранилищем ключей необходимо тщательно оберегать от несанкционированного доступа**.
- Пароль на доступ к ключу ЭП должен быть известен только Вам как владельцу.
- **Не допускайте постоянного и бесконтрольного подключения** к компьютеру аппаратных устройств с ключами ЭП.
- Не пользуйтесь Системой в интернет-кафе, ресторанах, транспорте (например метро) а также в других местах если вы не уверены в безопасности компьютеров или доступа в Интернет.
- Не подключайте к услугам Банка номера телефонов, которые Вам не принадлежат.
- Отключите использование идентификационных файлов (cookie) на сайте Банка либо после завершения работы в Системе Интернет-Банк удалите идентификационный файл (cookie) в Браузере (раздел «Настройки», подраздел «Безопасность», опция «Очистить журнал обозревателя/журнал браузера/cookie»)
- **При возникновении любых подозрений на компрометацию ключей ЭП** или обнаружении в компьютере вредоносных программ — обязательно сообщите в Банк и заблокируйте ключи ЭП.
- **При любых проявлениях необычного поведения Системы** или изменениях в интерфейсе программы – прекратите проведение операций в Системе и **срочно позвоните в Банк** и уточните причину. Если изменения не связаны с обновлением версии программного обеспечения, заблокируйте все ключи ЭП.

Предполагаемые категории мошенников

Хищение средств с расчетных счетов при получении доступа к 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 ключам ЭП, например, уволенные руководители, работники бухгалтерии и их заместители, бывшие владельцы компании.
- Штатные ИТ-сотрудники Вашей компании, имеющие или имевшие технический доступ к носителям с ключами ЭП и к компьютерам компании, подключенным к Системе.
- Внештатные, приходящие по вызову ИТ-специалисты сторонних организаций, обслуживающие компьютеры Вашей компании, осуществляющие профилактику и подключение к Интернету, установку и обновление бухгалтерских, информационно-правовых и других программ на компьютеры, подключенные к Системе.
- Другие злоумышленники, осуществляющие доступ к Вашим компьютерам путем заражения компьютеров через Интернет вредоносными программами и хищение ключей ЭП и паролей.

Таким образом, при отсутствии контроля за действиями указанных лиц, в Банк могут поступать не вызывающие подозрений платежи, направленные злоумышленниками с использованием действующих ключей ЭП, имеющие обычные реквизиты получателей и типовые назначения платежа.

АО КБ «Соколовский» напоминает Вам о том, что:

- Банк не имеет доступа к Вашим ключам ЭП и не может от Вашего имени сформировать корректную ЭП под электронным платежным документом.
- Банк никогда не осуществляет рассылку электронных писем с просьбой прислать Ваш 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 или паролей, срочно сообщите об этом в Службу технической поддержки клиентов Банка.

- Вы являетесь единственным владельцем ключей ЭП и ответственность за их конфиденциальность лежит на Вас.
- Если Вы сомневаетесь в конфиденциальности ключей ЭП или подозреваете компрометацию (копирование) данных, срочно заблокируйте ваши ключи ЭП.
- Изменение пароля доступа к ключу ЭП не защищает Вас от использования злоумышленниками ранее похищенного ключа. В этом случае необходимо заблокировать старый ключ и получить новый.

Требования по защите Рабочего места Системы Интернет-Банк от Вредоносного программного обеспечения

Вредоносное программное обеспечение (ВПО) - компьютерные программы, предназначенная для внедрения в автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование клиентов - пользователей систем дистанционного банковского обслуживания, приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.

К средствам защиты от ВПО относятся средства, осуществляющие:
- выявление и обезвреживание ВПО (антивирусы);
- межсетевое экранирования Рабочего места или корпоративной сети;
- Web-фильтрацию;
- обнаружение и предотвращение вторжений;
- контроль выполнения приложений.

Для обеспечения надлежащей защиты от последствий действий ВПО Клиент обязан:
- обеспечить непрерывное использование средств защиты от ВПО;
- обеспечить периодический контроль целостности системного, прикладного и специального программного обеспечения;
- еженедельно осуществлять проверку Рабочего места на наличие ВПО;
- обеспечить регулярное обновление средств защиты от ВПО, обновление прикладного программного обеспечения, установку пакетов обновления безопасности операционной системы;
- использовать лицензионное программное обеспечение или программное обеспечение, полученное исключительно из доверенных источников;
- осуществлять вход в сеть Интернет с Рабочего места исключительно для подключения к серверу Банка или обновления антивирусной программы, прикладного или системного программного обеспечения, или для подключения к иным доверенным серверам сети Интернет по вопросам, связанным с исполнением служебных обязанностей;
- предварительно на выделенном компьютере проверять съемные носители информации на наличие Вредоносного кода перед использованием на Рабочем месте.

ПОРЯДОК ДЕЙСТВИЙ КЛИЕНТА ПРИ ВЯВЛЕНИИ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

В случае выявления хищения денежных средств в Системе Интернет-Банк необходимо:

1) Зафиксировать данные расчетных документов, по которым совершено хищение, немедленно прекратить любые действия с электронными устройствами (далее –ЭУ): персональными компьютерами, ноутбуками, планшетными компьютерами и т.п., используемыми в качестве удаленного рабочего места для целей дистанционного управления денежными средствами Клиента, подключенными к Системе Интернет-Банк, обесточить их (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь все аккумуляторные батареи из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, Wi-Fi, и др.) или перевести в режим гибернации ("спящий" режим).

2) При отсутствии возможности обесточивания ЭУ, осуществить отключение по штатной процедуре и запротоколировать указанный факт.

3) При наличии технической возможности отозвать перевод с использованием иного ЭУ (отправить Отзыв или сообщение свободного формата по Системе Интернет-Банк с указанием номера, даты, суммы расчетного документа), после чего принять меры к блокировке Системы Интернет-Банк.

4) При отсутствии технической возможности отозвать перевод по Системе Интернет-Банк, немедленно обратиться в Банк по телефону с заявлением о блокировке ключей ЭП, приостановке исполнения платежа и возврате денежных средств.

5) Оперативно обратиться в Банк с письменным заявлением об отзыве платежа, возврате средств и блокировке ключей ЭП (Приложение №12 к Договору). Копия заявления должна быть направлена в Банк незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в Банк как можно оперативнее.

6) Проинформировать все банки, с которыми Клиент имеет договорные отношения, предусматривающие использование дистанционного банковского обслуживания, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.

7) Произвести фотосъемку ЭУ (с подключенными кабелями и иными периферийными устройствами), рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) ЭУ как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин, мастичная печать, пломбы и т.д.) и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры ЭУ, следует поместить его в непрозрачный пакет (мешок) и заклеить горловину. При необходимости ведения хозяйственной деятельности –задействовать другое ЭУ.

8) Предпринять меры для обеспечения сохранности и неизменности записей с внутренних и внешних камер систем видеонаблюдения, журналов систем контроля доступа, средств обеспечения и разграничения доступа в сеть Интернет (при наличии таковых) за максимальный период времени, как до, так и после даты совершения хищения средств.

9) Провести сбор записей с межсетевых экранов и других средств защиты информации, серверов баз данных и иных компонентов клиентского приложения Системы Интернет-Банк, систем авторизации пользователей (AD, NDS и т.д.), коммуникационного оборудования (включая АТС), ЭУ, используемых для управления денежными средствами через Систему Интернет-Банк, устройств, которые могут использоваться для удаленного управления указанными ЭУ.

10) При возможности, оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи для получения в электронной форме журналов соединений с Интернет с электронного устройства Клиента или из его локальной вычислительной сети как минимум за три месяца, предшествовавшие факту хищения денежных средств.

11) Не предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ, не отправлять ЭУ в сервисные службы ИТ для восстановления работоспособности.

12) Зафиксировать в протокольной форме значимые действия и события, в том числе имена лиц, имеющих доступ к ЭУ, действия с ЭУ, подключенными к Системе Интернет-Банк., предшествовавшие факту хищения денежных средств, подготовить объяснения Клиента (работников Клиента) об использовании ЭУ в целях, отличных от осуществления операций в Системе Интернет-Банк., посещаемых сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в Банк, посторонних лицах, побывавших в месте расположения ЭУ и т.д.

13) Все действия, указанные в п. 1, 7, 8, 9, 12 настоящего раздела необходимо производить коллегиально, протоколировать и документировать, в т.ч.с использованием фотосъемки. При невозможности осуществления коллегиальных действий (для индивидуальных предпринимателей или физических лиц, занимающихся частной практикой) отдельно зафиксировать данный факт.

14) Оперативно обратиться с заявлением в правоохранительные органы о возбуждении дела по факту хищения денежных средств (глава 21 УК РФ).

15) В случае невозможности отзыва расчетного документа из Банка по причине его исполнения, оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить копию заявления о возбуждении уголовного дела, либо копию талона, содержащего порядковый номер из книги учета сообщений о преступлениях, содержащую отметку правоохранительного органа о его приеме.

16) Копии вышеуказанных документов направить в Банк с приложением Справки по факту инцидента информационной безопасности в Системе Интернет-Банк, а также подтверждающих документов.

Для получения дополнительной информации по техническим вопросам Вы можете обратиться к нашим специалистам. Мы всегда рады Вам помочь.