Правила доступа корпоративных клиентов к услугам ДБО
с указанием мер информационной безопасности.

В АКБ «СОЮЗ» (ОАО) (далее – «Банк») для корпоративных клиентов используется система дистанционного банковского облуживания (далее – «ДБО») «Клиент-Банк» (разработчик системы - ООО "БСС", http://www.bssys.com/).

Риски клиентов при работе с системами ДБО, использующих сеть Интернет

В связи с увеличивающейся популярностью банковских операций на основе современных электронных технологий, в последнее время в ряде российских банков участились случаи хищения денежных средств с расчетных счетов клиентов путем совершения платежей с использованием систем дистанционного банковского обслуживания типа «Клиент-Банк».
Анализ выявленных ситуаций показал, что хищения денежных средств с расчетных счетов осуществляются:

- злоумышленниками путем заражения вредоносными программами компьютеров клиентов в связи с уязвимостью системного и прикладного ПО (операционные системы, Web-браузеры, почтовые клиенты и пр.) с последующим дистанционным похищением секретных ключей электронной подписи (далее – «ЭП») и паролей;
- приходящими по вызову, ИТ-специалистами, выполняющими профилактику и подключение компьютеров к сети Интернет, установку и обновление различного программного обеспечения на компьютерах, с которых осуществляется работа по системе дистанционного банковского обслуживания;
- в случае корпоративного ДБО, как работающими, так и уволенными ответственными сотрудниками организации, имевшими доступ к носителям секретных ключей ЭП (дискеты, флеш-диски, жесткие диски и пр.), а также доступ к компьютерам, с которых осуществлялась работа по системе дистанционного банковского обслуживания.

Как правило, действия злоумышленников направлены:

- на похищение файла с секретным ключом ЭП или копирования носителя с этим ключом;
- на похищение паролей доступа к Системе;
- на передачу в банк электронных платежных документов, заверенных похищенным ключом ЭП.

Документы, направляемые злоумышленниками с использованием действующих секретных ключей ЭП клиентов, могут не вызывать подозрений у сотрудников банков, поскольку такие документы имеют корректную ЭП, вполне обычные реквизиты получателей и типовое назначение платежа. Благодаря этому, полученные платежные документы признаются банками, поступившими от клиента – владельца расчетного счета, и банки обязаны их исполнять. Таким образом, происходит хищение злоумышленниками денежных средств со счетов клиентов. При этом вся ответственность за убытки полностью возлагается на клиентов как единственных владельцев секретных ключей ЭП.
С целью повышения безопасности и снижения указанных выше рисков при работе с системами ДБО АКБ «СОЮЗ» (ОАО) рекомендует следовать нижеприведенным требованиям. Следует понимать, что для работы в системах ДБО к компьютеру применяются повышенные требования безопасности.

Общие требования безопасности при работе в сети интернет:

- Своевременно обновлять операционную систему (установка патчей, критичных обновлений).
- Установить и своевременно обновлять на компьютере антивирусное программное обеспечение (ПО). Антивирусное ПО должно быть запущено и работать постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, удаление обнаруженного вредоносного ПО.
- При выходе в Интернет использовать сетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет. Запретить в межсетевом экране соединение с сетью Интернет по протоколам ftp, smtp. Разрешить соединения smtp только с конкретными почтовыми серверами, на которых зарегистрированы Ваши электронные почтовые ящики.
- Не давать разрешения неизвестным программам выходить в сеть Интернет.
- При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
- Не использовать права администратора при отсутствии необходимости. В повседневной практике входить в систему как пользователь, не имеющий прав администратора.
- Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.

Требования по обеспечению информационной безопасности при работе в системах ДБО

В целях обеспечения информационной безопасности при работе в системе «Клиент-Банк» Клиент наделяется следующими обязанностями:

- Ни в коем случае не отвечать на письма, якобы от имени Банка, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену.

- https://ibc.banksoyuz.ru прислать секретный ключ или пароль доступа к системе, а немедленно сообщить о подобном факте Администратору Системы в рабочие часы Банка по телефону: (495) 729-55-15. Банк информирует Вас, что не осуществляет рассылку электронных писем с просьбой прислать ключи ЭП или пароль. Банк не рассылает по электронной почте программы для установки на Ваши компьютеры.
- Осуществлять вход в систему «Клиент-Банк» только через корпоративный сайт Банка https://ibc.banksoyuz.ru. В случае отсутствия возможности подключения к сайту сообщить об этом Администратору Системы по телефону: (495) 729-55-15.
- Запретить доступ из сети Интернет к компьютерам, используемым для работы в систему «Клиент-Банк», отключить возможность терминального соединения на эти компьютеры.
- Хранить ключи ЭП на съемном носителе (дискеты, флеш-диски), а не на жестком диске компьютера. По окончании работы с системой «Клиент-Банк», извлекать эти съѐмные носители и убирать их в надежное хранилище, исключающее доступ к нему неуполномоченных лиц и повреждение материального носителя.

Банк информирует Вас, что вся ответственность за конфиденциальность Ваших секретных ключей ЭП полностью лежит на Вас, как единственных владельцах секретных ключей ЭП.

- Обеспечивать конфиденциальность использования пароля доступа к системе «Клиент-Банк»; пароль не требуется сотрудникам Банка для обслуживания Клиента и поддержки Системы в работоспособном состоянии.
- Пароль доступа следует хранить отдельно от самого носителя: не записывайте пароль доступа на этикетке или бирке носителя.

- Обязательно смените пароль в том случае, если он стал известен постороннему лицу. Не рекомендуем использовать в качестве пароля:

    - последовательности символов, состоящие из одних цифр (в том числе даты, номера телефонов, номера автомобиля и т.п.);
    - последовательности повторяющихся букв или цифр;
    - подряд идущие в раскладке клавиатуры или в алфавите символы;
    - имена и фамилии.
    - ИНН или другие реквизиты клиента.
- Не отлучаться от компьютера, пока в нем находится носитель, содержащий секретный ключ ЭП.
- Не записывать на носитель, содержащий секретный ключ, какую либо другую информацию.
- Обеспечить использование секретного ключа ЭП только ответственным сотрудником, уполномоченным на то соответствующим распорядительным документом.
- Никогда не передавать ключи ЭП ИТ-сотрудникам для проверки работы Системы, проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только лично владелец ключа ЭП должен подключить съемный носитель к компьютеру, убедиться, что пароль доступа к системе вводится в интерфейс клиентского АРМ Интернет/Клиент-Банк, и лично ввести пароль, исключая его подсматривание.
- В случае выявления явных или косвенных признаков компрометации ключей ЭП, незамедлительно уведомить Банк по телефону: (495) 729-55-15, либо лично явиться в Банк с целью блокирования скомпрометированных секретных ключей ЭП с последующей их заменой. К событиям, связанным с компрометацией ключей АСП относятся, включая, но не ограничиваясь, следующие:

    - утеря материального носителя, содержащего секретный ключ, в том числе с последующим обнаружением;
    - выход из строя материального носителя, содержащего секретный ключ, когда невозможно достоверно определить причину этого события (доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
    - обнаружение факта или угрозы использования (копирования) ЭП и/или пароля доступа к Системе с использованием ЭП неуполномоченными лицами (несанкционированная отправка электронных документов);
    - обнаружение ошибок в работе Системы, в том числе возникающих в связи с попытками нарушения информационной безопасности;
    - увольнение ответственного сотрудника Клиента, имевшего доступ к секретному ключу.
- Помимо указанных выше требований Банк рекомендует также:
- Исключить доступ к компьютерам, используемым для работы в системе «Клиент-Банк», посторонним лицам и персоналу предприятия, не уполномоченному на работу в системе «Клиент-Банк» и/или обслуживание компьютеров.
- На компьютерах, используемых для работы по Системе, исключить посещение всех Интернет-сайтов, кроме используемых для входа в Систему, а также исключить установку развлекательных и игровых программ.
- Использовать только лицензионное ПО (операционные системы, офисные пакеты и пр.), обеспечить автоматическое обновление системного и прикладного ПО.
- Контролировать время и IP-адрес предыдущего сеанса работы с системой «Клиент-Банк». Данная информация выводится при подключении к системе.
- Фиксировать IP-адреса, с которых клиенту разрешен доступ к системе «Клиент-Банк». Данная услуга бесплатная, для еѐ подключения или отключения необходимо заполнить соответствующее заявление.