Риски клиентов при работе в системе дистанционного банковского обслуживания (далее – «Система»)

За последнее время в ряде российских банков участились случаи хищения денежных средств с расчетных счетов корпоративных клиентов путем совершения платежей с использованием системы дистанционного банковского обслуживания. Анализ выявленных ситуаций показал, что хищения денежных средств с расчетных счетов осуществляются:

как работающими, так и уволенными ответственными сотрудниками предприятия, имевшими доступ к паролю доступа, секретным ключам, к компьютерам, с которых осуществлялась работа по системе дистанционного банковского обслуживания;

как работающими, так и уволенными IT-сотрудниками организации, а так же нештатными, приходящими по вызову, IT-специалистами, выполняющими профилактику и подключение к Интернет, установку и обновление бухгалтерских и справочных программ, установку и настройку другого программного обеспечения на компьютерах, с которых осуществляется работа по системе дистанционного банковского обслуживания;

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 и паролей, а также путем использования ложных (фальсифицированных) ресурсов сети Интернет с целью получения персональных данных и реквизитов банковских карт клиентов.

Как правило, действия злоумышленников направлены:

- на похищение секретных ключей;
- на похищение паролей доступа к Системе;
- на передачу в банк электронных платежных документов, заверенных похищенным ключом.

Документы, направляемые злоумышленниками с использованием действующих секретных ключей клиентов, могут не вызывать подозрений у сотрудников банков, поскольку такие документы имеют корректную электронную подпись, 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 с расчетных счетов клиентов. **При этом вся ответственность за убытки безусловно и полностью возлагается на клиентов как единственных владельцев секретных ключей.**

В целях повышения безопасности при работе с системой дистанционного банковского обслуживания «Банка Заречье» (АО) представляет комплекс требований и рекомендаций, выполнение которых позволит снизить указанные выше риски при работе в Системе.

Требования по обеспечению информационной безопасности при работе в Системе

В целях обеспечения информационной безопасности при работе в Системе Клиент обязан:

1. Хранить Ключи электронной подписи (далее по тексту – ЭП) только на внешнем носителе информации в недоступном для посторонних лиц месте (персональный сейф, металлический шкаф).
2. Соблюдать запрет на копирование ключей ЭП на жесткий диск компьютера, с которого осуществляется работа в Системе.
3. Не использовать в качестве пароля:

– последовательности символов, состоящие из одних цифр (в том числе даты, номера телефонов, номера автомобилей и т.п.);

– последовательности повторяющихся букв или цифр;

– идущие подряд в раскладке клавиатуры или в алфавите символы;

– имена и фамилии;

– ИНН или другие реквизиты клиента.

4. Использовать пароль, содержащий:

– не менее 6 символов;

– цифры, строчные и заглавные буквы;

– хотя бы 1 символ, не являющийся буквой или цифрой.

5. Менять пароль пользователя в операционной системе, а также в системе ДБО не реже одного раза в квартал.
6. Хранить пароль доступа к ключу ЭП отдельно от ключа ЭП. Запрещено записывать пароль доступа к секретному ключу на этикетке внешнего носителя.

7. Подключать внешний носитель, содержащий ключ ЭП, только в момент подписания электронных документов. Запрещено оставлять внешний носитель, содержащий ключ ЭП, постоянно подключенным к компьютеру.
8. Использовать внешний носитель, содержащий ключ ЭП, только для подписания электронных документов. Запрещено использовать внешний носитель, содержащий ключ ЭП, для каких-либо других целей, в частности, не хранить на нём информацию произвольного содержания, не относящегося к работе с системой ДБО.
9. Не копировать содержимое внешнего носителя, содержащего ключ ЭП, и не передавать его никому даже на короткое время.
10. Закончив работу в системе ДБО или прервав её (даже на несколько минут), необходимо извлечь внешний носитель, содержащий ключ ЭП, и убрать его в недоступное другим лицам место.
11. Обеспечить защиту АРМ от несанкционированного доступа, а также заражения вредоносным кодом (вирусами).
12. Применять на рабочем месте лицензионные средства защиты от вредоносного кода. Обеспечить регулярное обновление антивирусных баз и их поддержание в актуальном состоянии. При увольнении штатных IT-сотрудников, а также после любых действий внештатных IT-специалистов или других работников, выполнявших какие-либо операции с компьютерами, предназначенными для работы в системе ДБО, проводить проверку компьютеров на отсутствие вредоносных программ.
13. Размещать АРМ способом, не позволяющим производить визуальное наблюдение за экраном ЭУ и его клавиатурой, в том числе посредством системы видеонаблюдения и через оконные проемы.
14. Не работать с системой ДБО с компьютеров, которые располагаются в общественных местах (Интернет-кафе, салонах, киосках и т.д.).
15. Осуществлять постоянный контроль отправляемых платежных документов при работе с системой ДБО, а также за состоянием своего расчетного (банковского) счета.
16. В случае выявления признаков компрометации ключей ЭП или выявления вредоносного кода в компьютере, используемом для работы в системе ДБО, необходимо немедленно извлечь ключ ЭП, выключить компьютер и уведомить Банк по телефонам: **(843) 557-59-74, (843) 557-59-88 с 8 часов 00 минут до 17 часов 00 минут (в рабочие дни)**, либо лично явиться в Банк с целью блокирования скомпрометированных закрытых ключей ЭП с последующей их заменой.

К событиям, связанным с компрометацией ключей ЭП, в том числе, относятся:

– утеря (утрата) носителя ЭП, в том числе, с последующим его обнаружением;

– обнаружение факта или угрозы использования (копирования) ключей ЭП и/или пароля доступа к ключам ЭП неуполномоченными лицами (несанкционированная отправка электронных документов);

– обнаружение ошибок в работе системы ДБО, в том числе, возникающих в связи с попытками нарушения информационной безопасности;

– увольнение ответственного сотрудника, имевшего доступ к закрытому ключу ЭП ДБО.

17. Осуществлять работу на АРМ (автоматизированном рабочем месте) с использованием учетной записи с ограниченными правами, доступ к учетной записи с полными правами (администратора) защищать надежным паролем.
18. При обнаружении несанкционированных платежных операций или утрате доступа к системе ДБО без согласия клиента, немедленно уведомить Банк и написать уведомление в Банк об инциденте в порядке, установленном п.11.4 Условий, а также обратиться с соответствующим заявлением в правоохранительные органы.
19. Настроить сетевое оборудование, обеспечивающее доступ Клиента в сеть, или специализированное программное обеспечение (брандмауэр, прокси-сервер и т.п.) на блокировку сетевых пакетов, передаваемых с АРМ, применяемого для работы в Системе, на любые адреса, не относящиеся к Системе, системе доменных имён (Domain Name System), DHCP-серверу, службе каталогов (Active Directory и т.п.) и службам синхронизации времени, обновления установленного программного обеспечения, операционной системы и антивирусных баз.
20. Помнить и соблюдать меры безопасности при формировании расчетов в сети Интернет, быть внимательным при обращении к ссылкам на сервис ДБО Банка и сайта Банка. В случае, если был обнаружен: фишинговый сервис ДБО или фишинговый сайт Банка, а также если мошенники пытаются связаться по электронной почте или иным способом с требованиями о предоставлении персональных идентификаторов доступа к Системе, необходимо незамедлительно сообщить об этом в Банк.

21. До подключения к Системе оценить риски, связанные с использованием Системы, в соответствии с п.22 данных требований и, основываясь на проведенной оценке рисков, принять решение об использовании Системы или отказе от работы с ней.

22. Стороны осознают риски, возникающие при использовании Системы:

- риск изготовления Закрытого ключа и Сертификата или выдачи Логина и временного пароля для доступа в систему на неуполномоченное лицо;
- риск Компрометации Закрытого ключа;
- риск атаки на электронное устройство (персональный компьютер, ноутбук и иное рабочее место, используемое Уполномоченным лицом Клиента для дистанционного управления Счетом в рамках Системы), в том числе с использованием вредоносного кода с целью совершения операции без согласия Клиента;
- риск Компрометации Логина и Постоянного пароля;
- риск утраты доказательств совершения мошенничества в случае обнаружения факта использования электронного средства платежа без согласия Клиента.

В целях обеспечения информационной безопасности при работе в Системе также рекомендуется:

1. Использовать только лицензионное программное обеспечение – операционные системы, средства защиты от вредоносного кода, офисные пакеты и т.д. (далее по тексту – ПО).
2. Обеспечить возможность своевременного обновления системного и прикладного ПО.
3. Выделить стационарный компьютер только для работы с системой ДБО.
4. Доступ в помещение, где размещен компьютер с системой ДБО, рекомендуется предоставлять только уполномоченным лицам.
5. Компьютер, с которого осуществляется подготовка и отправка электронных документов в Банк, не использовать в других целях, в том числе рабочих.
6. С целью обеспечения безопасности платежей рекомендуется использовать услугу SMS–информирования.
7. Исключить доступ к компьютерам, используемым для работы по Системе, посторонним лицам и персоналу предприятия, не уполномоченному на работу по Системе и/или обслуживание компьютеров.
8. При обслуживании компьютера IT-сотрудниками обеспечивать контроль над выполняемыми ими действиями.
9. Настроить аудит событий, регистрирующий возникающие ошибки работы операционной системы и приложений, вход пользователей и запуск программ, периодически просматривать журналы аудита, реагировать на ошибки и попытки несанкционированного доступа.