КОММЕРЧЕСКИЙ БАНК

«РЕСПУБЛИКАНСКИЙ КРЕДИТНЫЙ АЛЬЯНС»

(общество с ограниченной ответственностью)

Рекомендации по информационной безопасности

при работе с системой дистанционного банковского обслуживания для клиентов Банка

1. Введение

Анализ выявленных в Российской Федерации за последнее время попыток хищения денежных средств с расчетных счетов корпоративных клиентов, путем совершения платежей с использованием систем электронного банкинга показал, что хищения денежных средств с расчетных счетов осуществляются, как правило:

- ответственными сотрудниками предприятия, имевшими доступ к секретным (закрытым) ключам ЭП, в том числе работающими или уволенными (директорами, бухгалтерами и их заместителями);
- штатными ИТ-сотрудниками организаций, имевшими доступ к носителям с секретными (закрытыми) ключами ЭП, а также доступ к компьютерам, с которых осуществлялась работа по системе "Интернет-банкинг";
- нештатными ИТ-специалистами других компаний, выполняющими профилактику и подключение к Интернет, установку и обновление бухгалтерских и справочных программ, установку и настройку другого программного обеспечения на компьютеры, с которых осуществляется работа по системе "Интернет-банкинг";
- злоумышленниками путем заражения компьютеров клиентов или взятия под контроль с использованием уязвимостей системного и прикладного ПО (операционные системы, Web-браузеры, почтовые клиенты и пр.) с последующим дистанционным похищением секретных (закрытых) ключей ЭП и паролей.

Во всех выявленных случаях злоумышленники тем или иным образом получали доступ к секретным (закрытым) ключам ЭП и паролям и направляли в банки платежные поручения с корректной электронной цифровой подписью.

В связи с этим Банк информирует Вас о необходимости строгого соблюдения приведенных в данном документе рекомендаций по информационной безопасности.

2. Общие понятия

Информационная Безопасность – совокупность организационных и технических мер, направленная на повышение безопасности использования ИТ технологий. Далее по тексту **ИБ**.

Система Дистанционного Банковского Обслуживания – совокупность сервисов дистанционного обслуживания «Интернет-банкинг». Далее по тексту используется сокращение **ДБО**.

ПО – программное обеспечение.

Вредоносное ПО - это разного рода программы (в том числе вирусные). Такие программы могут регистрировать последовательность нажимаемых на клавиатуре клавиш, другие делают снимки экрана при посещении пользователем сайтов, предлагающих банковские услуги, третьи загружают на компьютер дополнительный вредоносный код, предоставляют хакеру удаленный доступ к компьютеру и т.д. Все эти программы объединяет то, что они позволяют злоумышленникам собирать конфиденциальную информацию и использовать ее в том числе для кражи денег у пользователей.

ЭП (электронная подпись) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) и которая используется для определения лица, подписывающего информацию.

3. Важные замечания

Важно понимать, что:

- Банк не имеет доступа к секретным ключам ЭП и паролям Клиентов для доступа в систему дистанционного банковского обслуживания.
- Банк не может от имени Клиента сформировать ЭП под электронным платежным поручением.
- Вся ответственность за конфиденциальность секретных (закрытых) ключей ЭП полностью лежит на Клиенте, как на единственном владельце секретных (закрытых) ключей ЭП.
- Банк не рассылает по электронной почте и не озвучивает по телефону секретный ключ ЭП или пароль Клиента.

- Банк не запрашивает по электронной почте и по телефону секретный ключ ЭП или пароль, а также номер банковской карты Клиента и ПИН-коды.
- Если Клиент сомневается в конфиденциальности своих секретных (закрытых) ключей ЭП или есть подозрение в их компрометации (копировании), Клиент должен заблокировать свои ключи ЭП обратившись в Банк.

4. Меры информационной безопасности

4.1. Организационные меры клиента Банка.

Для снижения риска неправомерного доступа к системе ДБО «Интернет-банкинг» и информирования об ограничениях способов и мест использования, случаях повышенного риска использования электронного средства платежа, клиенту Банка (Юридическое лицо, Индивидуальный предприниматель) необходимо определить:

- ограниченный перечень лиц имеющих доступ к системе ДБО и ЭП;
- правила хранения и использования носителей ЭП;
- перечень событий, наступление которых должно повлечь за собой немедленную замену или изъятие ключей ЭП.

Клиенту Банка необходимо предупредить своих ответственных сотрудников об увеличении риска хищения и дальнейшего неправомерного использования ЭП при доступе к системе «Интернет-банкинг» с гостевых рабочих мест в местах общего пользования. В перечне таких мест могут быть Интернет-кафе, организации быстрого питания, офисы других организаций, крупные транспортные узлы, гостиницы и другие предприятия сферы услуг с открытыми сетями WiFi.

4.2. Правила безопасного использования сети Интернет.

- На компьютерах, используемых для работы с системой "Интернет-банкинг", исключить посещение интернет сайтов сомнительного содержания, загрузку и установку нелицензионного ПО и т. п.
- При регистрации на сайтах, нельзя указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.
- Если пришло сообщение с незнакомого адреса **(включая сообщения электронной почты; мессенджеров ICQ, Skype и т.п.; Социальных сетей**), его лучше не открывать. Подобные письма могут содержать вирусы.

- Нежелательные письма от незнакомых людей называются **«Спам».** При получении такого письма, не отвечать на него. В случае ответа на подобное письмо, отправитель будет знать, что данный электронный почтовый ящик активно используется, и будет продолжать посылать на этот адрес спам.
- При скачивании контента надо внимательно читать условия использования сервиса, а также информацию, размещенную с символом «звездочка» (*)
- Необходимо быть осторожным при всплывающих окнах и не переходить по неизвестным ссылкам и адресам.
- Не отправлять SMS для разблокировки Windows и разархивирования файлов.

4.3. Доступ к компьютеру и его защита.

- Необходимо ограничить доступ к компьютеру, на котором установлен Интернет-банкинг. Доступ к компьютеру должны иметь только уполномоченные сотрудники. Рекомендуется регулярно менять пароль на вход в операционную систему, на которой установлен Интернет-банкинг.
- При обслуживании компьютера ИТ-сотрудниками сторонней организации необходимо обеспечивать контроль над выполняемыми ими действиями.
- Необходимо убедится, что компьютер с установленной системой ДБО не поражен какими-либо вирусами. Необходимо установить и активировать антивирусные программы, обеспечить возможность автоматического обновления антивирусных баз, а так же еженедельно проводить антивирусную проверку. Обратите внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о вашем пароле и ключах ЭП.
- Рекомендуется установить и использовать персональный брандмауэр (firewall) на компьютерах с доступом в интернет, это позволит предотвратить несанкционированный доступ к информации на компьютере.
- Необходимо использовать лицензионное программное обеспечение (в том числе антивирусное), межсетевые экраны и средства защиты от несанкционированного доступа.
- При смене ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с системой "Интернет-банкинг", необходимо принять

меры по смене паролей с правами администратора и провести проверку на отсутствия вредоносных программ на компьютерах.

- **При увольнении сотрудника, имеющего доступ к паролям и ключам ЭП, необходимо произвести смену паролей, блокировать ЭП с которой работал уволенный сотрудник, и получить ЭП для нового сотрудника.**

4.4. Правила работы в системах ДБО.

4.4.1. Пароли.

- Не использовать для защиты данных очевидные пароли, которые легко угадать: имя супруга (супруги), ребенка, домашнего животного, номера телефонов, регистрационный номер машины, почтовый индекс и т.п.;
- Не сообщать никому свой пароль. Если с вами связался (например, по телефону) представитель некой организации и попросил сообщить ваш пароль, не раскрывайте свои личные данные: вы не знаете, кто на самом деле находится на другом конце провода;
- Не записывать логин и пароль на бумаге или в файлы на рабочем компьютере. В случае необходимости хранения параметров доступа на бумажном носителе, пароли необходимо хранить в запечатанных конвертах или в сейфе вместе с ключами ЭП. Недопустимо расположение паролей на бумажных носителях на рабочем столе, под клавиатурой и т.п.;
- Не вводить электронную подпись и пароль Интернет-банкинга на компьютерах, которые находятся в общедоступных местах (например: интернет кафе);
- Не использовать одинаковый логин и пароль для доступа к различным системам;
- При смене паролей не допускать повторяющиеся и схожие пароли (например: пароль1, пароль2, пароль3 и т.п.)
- Не допускается хранить пароль для входа в систему ДБО в файле на локальном диске, либо в любом другом легкодоступном месте. Необходимо убедиться, что только уполномоченные сотрудники могут получить доступ к паролю для входа в систему. **Если возникли подозрения, что кто-либо владеет информацией о пароле, необходимо самостоятельно сменить пароль или заблокировать его**

с помощью обращения в Банк по телефону. Так же заблокировать пароль можно в офисе банка, написав соответствующее уведомление.

4.4.2. Ключи Электронной подписи.

Необходимо серьезно отнестись к вопросу хранения ключей Системы ДБО. Наличие ключа позволяет заверить от имени владельца документ и передать его на исполнение в Банк. Для повышения безопасности рекомендуется:

- Использовать для хранения файлов с секретными (закрытыми) ключами ЭП только отчуждаемые носители: USB-токены, к которым исключен доступ третьих лиц.
- Использовать устройства защищенного хранения закрытых ключей ЭП - USB-токены (безопасность обеспечивается наличием защищенного хранилища данных, доступ к которому возможно только владельцем USB-токена, знающим PIN-код ключа).
- Не передавать ключи ЭП ИТ-сотрудникам для проверки работы системы "Интернет-банкинг", проверки настроек взаимодействия с банком и т.п. При необходимости таких проверок только владелец ключа ЭП, лично, должен подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского части системы ДБО, и лично ввести пароль.
- Выходить из системы "Интернет-банкинг" и отключать носитель ЭП, даже если надо отойти от компьютера на несколько минут.

4.4.3. Контроль подключения (для сервиса «Интернет-Банкинг»).

- Необходимо проверять, что соединение действительно происходит в защищенном режиме. В этом случае адресная строка в браузере начинается с **https://**, а в адресной строке и правом нижнем углу вэб-браузера должен быть виден **значок закрытого замка**.
- Необходимо убедиться в том, что соединение установлено именно с сайтом системы "Интернет-банкинг".
- Необходимо контролировать посещения системы, проверяя дату последнего посещения и IP-адрес, отображаемые на главной странице

- Регулярно проверять состояние счетов и движение документов по выпискам.
- Не вводить конфиденциальные данные, если окно для ввода отличается от стандартных окон Системы «Клиент-Банкинг» (другие надписи, шрифт и тому подобное) или отображается не так как всегда (нарушен порядок работы в системе). О появлении подобных сайтов немедленно сообщите в Банк по телефону. Так же заблокировать доступ в систему ДБО можно в офисе банка, написав соответствующее уведомление.
- После окончания работы в системе ДБО надо всегда использовать пункт меню «Выход».

4.5. Случаи, требующие немедленного обращения в Банк.

Незамедлительно надо обратиться в Банк, если:

- Возникло подозрение, что пароль или секретные ключи были скомпрометированы, а также, если была обнаружена иная подозрительная активность в системе ДБО.
- За сменой электронной подписи, в случае увольнения/ухода уполномоченных сотрудников или сотрудников IT клиента, которые имели доступ к ним.
- При возникновении любых подозрений на компрометацию (копирование) секретных (закрытых) ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ). В случае выявления подозрительной активности на компьютере с установленной системой "Интернет-банкинг" (самопроизвольные движения мышью, открытие/закрытие окон, набор текста) немедленно надо выключить компьютер и сообщить в Банк о возможной попытке несанкционированного доступа к системе**.**

5. Заключение

5.1. Настоящие Рекомендации вступают в силу с момента их утверждения Председателем Правления Банка и действуют до их отмены.

5.2. В настоящие Рекомендации могут быть внесены изменения, дополнения в установленном в Банке порядке.