Памятка

по обеспечению безопасности работы систем дистанционного банковского обслуживания

ООО «Банк РСИ» придает большое значение обеспечению безопасности доступа к средствам Клиентов. Пожалуйста, внимательно прочитайте нижеизложенную информацию и следуйте нашим рекомендациям.

В последнее время в банках участились попытки хищения денежных средств со счетов юридических лиц, использующих системы дистанционного банковского обслуживания.

Обратите внимание! Согласно статистике, наиболее часто попытки хищения средств осуществляются:

- **сотрудниками организаций,** в том числе уволенными, имеющими или имевшими доступ к СКЗИ JaCarta ГОСТ, а также доступ к компьютерам, с которых осуществляется работа с системой ДБО;
- **ИТ-специалистами (штатными и внештатными)**, оказывающими (или оказывавшими ранее, в т.ч. однократно) различные ИТ-услуги по поддержке, подключению к сети Интернет, установке, обновлению и поддержке различных программ (бухгалтерских, правовых, информационных и др.) на компьютерах, с которых осуществляется работа с системой ДБО;
- **мошенниками**, с использованием сети Интернет, путем заражения компьютеров различными вирусами и вредоносным программным обеспечением (используя «бреши» в безопасности компьютеров и корпоративной сети организации), с последующим хищением через Интернет ключей ЭП и средств доступа к системе ДБО.

Во всех перечисленных случаях мошенники, завладев ключами ЭП и средствами доступа к системе ДБО Клиента, направляют от его имени в банк различные платежи в адрес физических и юридических лиц.

После того, как Банк передал Вам средства доступа к системе ДБО (логин/пароль) и ключи электронной подписи (ЭП), конфиденциальность полученных Банком данных по системе ДБО полностью зависит от того насколько ответственно Вы отнесётесь к их использованию и хранению, а также к защите компьютеров, с которых осуществляется работа с системой ДБО.

Для снижения риска несанкционированного доступа к системе ДБО рекомендуем Вам осуществить следующие организационные и технические меры:

1. **Обеспечить безопасность** СКЗИ JaCarta ГОСТ**, используемых в системах ДБО:**

1.1. Для хранения ключей ЭП использовать только СКЗИ JaCarta ГОСТ, а не жёсткие/сетевые диски компьютера. Доступ к СКЗИ JaCarta ГОСТ должен быть строго ограничен: лица, обладающие правом подписи на документах, бухгалтер, работающий с системой ДБО по доверенности - далее «уполномоченные лица».

Хорошей практикой является хранение вышеуказанных носителей в сейфе в опечатанном контейнере. Целостность печати (пломбы) должна ежедневно, в начале рабочего дня, контролироваться руководителем организации или уполномоченным лицом. После завершения работы ключевой носитель помещается в контейнер и заново опечатывается (пломбируется) уполномоченным лицом.

1.2. Не использовать СКЗИ JaCarta ГОСТ для каких-либо других целей (в частности, не хранить на них любую другую информацию).

1.3. Извлекать СКЗИ JaCarta ГОСТ из компьютера каждый раз после завершения их использования (т.е. СКЗИ JaCarta ГОСТ должны находиться в компьютере только в момент подписания) – даже если работа в системе ДБО продолжается, носители должны быть извлечены из компьютера сразу после окончания подписания документов.

Не допускать (даже на минимальное время) нахождение СКЗИ JaCarta ГОСТ:

- *установленными в компьютер, если Вы их не используете;*

– *в открытом доступе (например, на столе) в тот момент, когда они не находятся в зоне «прямой видимости» – в случае необходимости отлучиться от рабочего места поместите СКЗИ JaCarta ГОСТ в защищённое место (например, в сейф).*

1.4. Не передавать СКЗИ JaCarta ГОСТ кому-либо, в том числе ИТ-специалистам для проверки работы системы, настроек взаимодействия с Банком и т.п. При необходимости таких проверок владелец ЭП обязан лично подключать СКЗИ JaCarta ГОСТ к компьютеру.

2. Обеспечить безопасность средств доступа (логин/пароль), используемых в системе ДБО:

2.1. Не допускать использования простых паролей (123456, qwerty и др.) – использовать различные сложные комбинации из букв (в т.ч. в разных регистрах) и цифр, не расположенных «подряд» на клавиатуре.

2.2. Осуществлять регулярную (минимум – 1 раз в месяц) смену паролей, используемых в системе ДБО.

2.3. Не назначать пароль, используемый в системе ДБО, в любых других системах и сервисах.

2.4. Не сообщать логин или пароль, используемый в системе ДБО, кому-либо, в том числе ИТ-специалистам для проверки работы системы, настроек взаимодействия с Банком и др. При необходимости таких проверок владелец средств доступа обязан лично вводить свои логин и пароль в системе ДБО.

Не записывайте пароли на бумажных листках или в текстовых файлах на компьютере, не оставляйте их в легкодоступных местах (на рабочем столе), не передавайте их третьим лицам. Если есть необходимость – храните все пароли, записанными на одном листе, в сейфе, в опечатанном контейнере вместе с ключевым носителем.

Рекомендуем Вам незамедлительно сменять пароль и осуществлять перегенерацию ключей ЭП (используя соответствующие возможности системы ДБО) или обращаться в Банк за выдачей новых средств доступа и ключей ЭП в следующих случаях:

– *при смене, увольнении сотрудника, имевшего даже потенциально доступ к ключевому носителю ЭП;*

– *при возникновении любых подозрений на компрометацию (копирование) ключей ЭП и/или средств доступа;*

– *в случае обнаружения каких-либо вредоносных программ на компьютере, используемом для работы в системе ДБО.*

3. На компьютере, с которого осуществляется работа с системой ДБО:

3.1. Физический доступ к компьютеру предоставлять только уполномоченным лицам. Рекомендуется использовать следующие методы защиты физического доступа к компьютеру:

– опечатать системный блок компьютера пломбой (или голографической наклейкой, стикером), целостность пломбы (наклейки, стикера) регулярно контролируется уполномоченным лицом;

– установить пароль **BIOS** на включение компьютера и на вход в настройки **BIOS**;

– выполнять вход в Windows путем ввода имени пользователя и его пароля;

– не допускать использования «пустых» или простых паролей (123456, qwerty, и пр.) для всех учетных записей, имеющих право входа в Windows, а также осуществлять периодическую смену паролей (рекомендуемая частота смены паролей – 90 дней);

– заблокировать учетную запись пользователя «Гость» (**«guest»**);

– не допускать работу под учетной записью Windows, имеющей права администратора – необходимо использовать учетную запись с ограниченными правами в операционной системе Windows, установленной на компьютере, используемом для работы с системой ДБО. Рекомендуется использовать разрешения **файловой системы NTFS,** а именно: предоставить полный доступ к папке (и всем вложенным в нее папкам и файлам), в которой находятся программные модули системы ДБО,

пользователю, работающему с системой ДБО, и указать **явный запрет** на доступ к этой папке для всех остальных пользователей;

– на компьютере с установленной системой ДБО **остановить и запретить для запуска службу Server, остановить и запретить службу удаленного управления реестром** Windows. Это приведет к невозможности доступа к компьютеру с установленной системой ДБО по сети, что, повлечет однако ряд ограничений: на этом компьютере нельзя будет создавать общие сетевые папки и предоставлять доступ к его локальному принтеру по сети для других компьютеров Вашей организации.

Тем не менее, применение этой меры является необходимым, так как оно обеспечивает (при условии соблюдения пп. 3.3, 3.5) сетевую информационную безопасность персонального компьютера, используемого для работы с системой ДБО;

– включить на компьютере с установленной системой ДБО системный аудит, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал событий и реагировать на ошибки;

– наблюдать за всеми действиями сотрудников (в т.ч. ИТ-специалистов, администраторов), в течение всего времени выполнения ими каких-либо действий на компьютерах, используемых для работы с системой ДБО. Администратор (ИТ-специалист) должен подробно объяснять уполномоченному лицу, какие действия и с какой целью он выполняет в настоящее время.

3.2. Обеспечивать своевременную (по возможности, автоматическую, используя Windows Update) загрузку и установку всех последних обновлений от Microsoft, а также регулярное обновление другого системного и прикладного программного обеспечения по мере появления их новых версий.

3.3. Установить и регулярно автоматически обновлять лицензионное антивирусное программное обеспечение и его баз. Монитор антивируса должен быть постоянно включен с момента загрузки компьютера. Должно быть настроено регулярное автоматическое сканирование оперативной памяти и жестких дисков компьютера на наличие вирусов.

3.4. Применять специализированные программные средства безопасности: персональные межсетевые экраны (файрволы), антишпионское программное обеспечение и другое специализированное программное обеспечение, использующееся для обеспечения ИТ-безопасности, которое должно регулярно обновляться и правильно настраиваться.

При настройке персонального межсетевого экрана необходимо заблокировать несанкционированный исходящий и входящий трафик по всем TCP и UDP портам для всех адресов, как Интернет, так и внутренней локальной сети организации (настроить персональный экран по принципу: запрещено все, что не разрешено), запретить работу по протоколам ftp и smtp, разрешить доступ только к необходимым ресурсам (в частности, к используемым системой ДБО).

При наличии в Вашей организации грамотного системного администратора возможна более тонкая настройка файрвола – открытие определенных портов и адресов для правильного взаимодействия компьютера, например, с контроллерами домена, запрет на установку и исполнение любых несанкционированных программ (отслеживание вирусных атак на компьютер) и т.д.

Если в Вашей организации уже есть развернутая программная или аппаратная система сетевого экранирования, защищающая периметр сети, то включение собственного файрвола на компьютере (при условии правильной его настройки и регулярном обновлении), все равно, является обязательным требованием – это Ваш последний рубеж обороны.

Более подробную информацию по п.п. 3.2 – 3.4 Вы можете получить на сайте Microsoft:

http://www.microsoft.com/Rus/Security/Protect/Default.mspx
http://www.microsoft.com/Rus/Protect/Computer/default.mspx

3.5. Рекомендуется не посещать посторонние Интернет-сайты (не относящиеся к системе ДБО), сайты сомнительного содержания, не работать с электронной почтой (особенно через общедоступные почтовые Web-сервера: Mail.ru и т.д.), устанавливать и использовать нелицензионное программное обеспечение, программы мгновенных почтовых сообщений (ICQ, QIP и т.д.), запрещается пользоваться Skype, устанавливать игры и любые программы с пиратских дисков, просматривать видеофильмы, слушать музыку, загружать и устанавливать любые программы из Интернет, открывать и редактировать непроверенные антивирусом DOC, XLS, PDF файлы.

Внимание! Компьютер, который используется для работы с ДБО должен обслуживаться грамотным системным администратором, на нем должны выполняться следующие регулярные работы: проверка успешности функционирования антивирусного программного обеспечения и файрвола, полное сканирование компьютера антивирусом, обновление антивируса и файрвола, установка необходимых обновлений операционной системы (установка патчей, критичных обновлений системы безопасности Windows). Во время проведения этих работ ключевой носитель должен находиться в сейфе!

НАСТОЯТЕЛЬНО ПРОСИМ ВАС НЕЗАМЕДЛИТЕЛЬНО ОБРАЩАТЬСЯ В БАНК ПРИ ВОЗНИКНОВЕНИИ СЛЕДУЮЩИХ СИТУАЦИЙ:

- У Вас не работает система ДБО по неизвестным («необычным») причинам (например, не запускается операционная система Windows, Вы не можете войти в систему ДБО, т.к. возникает «ошибка авторизации», говорящая о неправильно набранном пароле, хотя пароль Вы набираете на клавиатуре верно или вход в систему заблокирован, невозможно связаться с банковским сервером системы ДБО, необычная работа известных программ и т.п.).
- Обнаружены (или есть подозрения на несанкционированный доступ к Вашей информации) факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время и т.п.).
- В выписке обнаружены несанкционированные Вами расходные операции.

Обращаем Ваше внимание, что своевременное обращение в Банк позволит принять оперативные меры по предотвращению мошенничества и сохранить Ваши средства.