ПАМЯТКА О МЕРАХ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С СИСТЕМОЙ ДБО

Подсистема «Интернет-Клиент»

Электронная почта: dbo@bcosm.ru

Многоканальный телефон АО КБ «КОСМОС»: +7 (495) 792-88-92

АО КБ «КОСМОС» доводит до сведения Клиентов – пользователей дистанционного банковского обслуживания (ДБО) счетов через системы «Банк-Клиент» и «Интернет-Клиент» информацию о том, что данная банковская услуга как способ распоряжения счетом содержит в себе определенные риски. Соблюдение нижеследующих мер безопасности позволит Вам избежать случаев хищения мошенниками денежных средств со счетов Вашей компании.

1. Обеспечение безопасности Средств Доступа и носителей с ключами ЭЦП, используемых в системе ДБО:

Максимальную безопасность при работе со счетом с использованием системы ДБО достигается с использованием следующих правил:

1.1. РАБОТА С ЛОГИНОМ И ПАРОЛЕМ

1.1.1. Логин – средство доступа, полученное в Банке, его изменение невозможно.

1.1.2. При первом входе в систему ДБО обязательно смените пароль, для чего пройдите следующий путь:

- в системе «Интернет-Клиент»: ***«Сервис – Безопасность – Смена пароля»***.

1.1.3. Не допускайте использования простых паролей (123456, qwerty и др.) – используйте различные сложные комбинации из букв (в т.ч. в разных регистрах) и цифр, не расположенных «подряд» на клавиатуре (например: s84@d*8V).

1.1.4. Осуществляйте регулярную (минимум 1 раза в месяц) смену паролей, используемых в системе ДБО – это самый действенный способ снизить вероятность несанкционированного доступа к счету.

1.1.5. Не назначайте пароль, используемый в системе ДБО, в любых других системах и сервисах.

1.1.6. Не сообщайте логин или пароль, используемый в системе ДБО, кому-либо, в том числе IT-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.

Рекомендуем Вам незамедлительно сменять пароль и осуществлять перегенерацию ключей электронной цифровой подписи (ЭЦП), (используя соответствующие возможности системы ДБО) или обращаться в Банк за заменой Средств Доступа и ключей ЭЦП:

- при увольнении сотрудника, имевшего доступ к ключам ЭЦП;

- при возникновении любых подозрений на компрометацию (копирование) ключей ЭЦП и/или Средств Доступа;

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

1.2. РАБОТА С НОСИТЕЛЯМИ ЭЦП

1.2.1. Для доступа к системе ДБО в Банке Вам был выдан защищенный носитель криптографической информации JaCarta-2 ГОСТ.

1.2.2. Существует два варианта работы с системой ДБО:

- Полный – включает возможность составления, подписания ЭЦП и отправки в Банк электронного платежного документа.

- Ограниченный – включает возможность составления электронного платежного документа без возможности отправки электронного платежного документа в Банк.

1.2.3. По каждому из вышеописанных вариантов определите своим приказом круг уполномоченных на работу в системе ДБО лиц. Предоставьте в Банк приказ и заполненные списки (приложение к договору ДБО) на каждое уполномоченное Вами лицо. После выполнения указанной процедуры Банк выдаст Вам средство доступа к системе ДБО на каждое указанное в списке(ах) лицо, в соответствии с предоставленными ему приказом полномочиями.

1.2.4. Носитель ЭЦП должен храниться только у лица, которому он был выдан в соответствии со списком.

1.3. РАБОТА С СИСТЕМОЙ ДБО

1.3.1. Используйте для хранения ключей ЭЦП только защищенные носители, выданные Банком, а не жёсткие/сетевые диски компьютера, флеш носители. При этом владелец такого внешнего носителя должен хранить его в условиях, исключающих доступ к нему третьих лиц (например, использовать для хранения личный сейф).

1.3.2. Не используйте носители с ключами ЭЦП для каких-либо других целей (в частности, не храните на них любую другую информацию), например, ключи для доступа в ДБО других Банков.

1.3.3. Не используйте для работы в системе Интернет-Банк гостевые рабочие места (интернет-кафе, гостиницы и др.) – это увеличивает риск хищения ключа ЭЦП и другой информации, имея которую злоумышленники могут похитить денежные средства с Вашего счета.

1.3.4. Носители с ключами ЭЦП должны находиться в компьютере в течение ограниченного времени, необходимого и достаточного для непосредственной работы со счетом (просмотр выписок, подготовка платежных поручений, отправка платежей).

Не допускайте (даже на минимальное время) нахождение носителей с ключами ЭЦП:

- 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 носители с ключами ЭЦП в защищённое место (например, в личный сейф).

1.3.5. Для проверки работы системы ДБО, настроек взаимодействия с Банком не передавайте ключи ЭЦП кому-либо, в том числе IT-специалистам, при осуществлении проверки владелец ЭЦП обязан лично вводить логин и пароль и подключать носитель с ключами ЭЦП к компьютеру. При необходимости таких проверок безопаснее всего обратиться в службу поддержки Банка,

1.3.6. Каждый раз при работе с системой ДБО алгоритм Ваших действий в целях безопасности должен выглядеть следующим образом:

- проверка и визуальный осмотр носителей ЭЦП (носители ЭЦП должны находиться в том месте где Вы их оставили после последнего сеанса работы с системой ДБО, на них не должно быть каких-либо внешних повреждений – царапин, сколов, следов залития жидкостью и т.п., которых не было вовремя Вашего последнего сеанса работы с ними) в случае наличия сомнений в том, что носитель мог использоваться без Вашего ведома, не используйте его и незамедлительно обратитесь в Банк;

- вход в систему ДБО посредством ввода Вашего логина и пароля и SMS кода;

- проверка выписки платежей по счету до начала работы с системой ДБО, с целью убедиться в отсутствии несанкционированных Вами платежей (в случае возникновения сомнений в правильности или легитимности платежа немедленно прекратите работу с системой ДБО и свяжитесь со службой тех. поддержки Банка);

- работа с системой ДБО (формирование, подписание ЭЦП и отправка электронных платежных документов);

- по окончанию работы с системой ДБО осуществите выход из системы ДБО, извлеките из компьютера средство доступа к системе ДБО и поместите его в защищенное место.

1.3.7. По окончанию рабочего дня войдите в систему ДБО и осуществите проверку выписки платежей по счету, с целью убедиться в отсутствии несанкционированных Вами

платежей (в случае возникновения сомнений в правильности или легитимности платежа немедленно прекратите работу с системой ДБО и свяжитесь со службой тех. поддержки Банка).

В большинстве случаев возможный возврат несанкционированно списанных денег более вероятен при максимально быстром обнаружении мошеннического платежа.

2. Обеспечение безопасности компьютера, с которого осуществляется работа с системой ДБО

Получив в Банке комплект для работы с системой ДБО, и установив его на свой компьютер, помните, что с этого момента компьютер – это средство управления Вашим счетом, в связи с этим ему необходимо обеспечить надлежащую охрану, а именно:

2.1. Применять средства антивирусной защиты, обеспечивая при этом регулярное обновление антивирусных баз, а также еженедельную полную антивирусную проверку.

2.2. Применять специализированные программные средства безопасности: персональные файрволы (Personal Firewall), антишпионское программное обеспечение (Anti-Malware software) и другое специализированное ПО, использующееся для обеспечения IT-безопасности.

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

2.4. Использовать компьютер, с которого осуществляется работа с системой ДБО только для работы в системе «Интернет-Клиент», избегать установки на него посторонних программ, игр, хранения на нем музыкальных и видео файлов, «закачивания» файлов из сети Интернет, посещения

Интернет сайтов сомнительного содержания, могущих содержать вредоносное программное обеспечение, любых выходов в сеть Интернет кроме как для работы с системой ДБО.

2.5. Осуществлять антивирусную проверку любых файлов и программ, загружаемых из сети Интернет либо полученных по электронной почте или на внешних носителях (дискеты, флеш-накопители, CD/DVD и др.).

2.6. Ограничивать доступ к компьютеру персонала, не имеющего отношения к работе с системой ДБО.

2.7. Не допускать работу под учётной записью Windows, имеющей права администратора - необходимо использовать учётную запись с ограниченными правами в операционной системе Windows, установленной на компьютере.

2.8. Не допускать использования «пустых» или простых паролей (123456, qwerty и др.) для всех учётных записей, имеющих право входа в Windows, а также осуществлять периодическую смену паролей (рекомендуемая частота смены паролей – 1 раз в месяц).

2.9. Запрещать использование любых средств удалённого (дистанционного) доступа, которые обычно используется IT-специалистами для удалённой (дистанционной) поддержки. Заблокировать возможность использования таких средств с помощью файрвола (программного и/или аппаратного).

2.10. Степень защиты компьютера, на котором установлена система ДБО, в значительной мере, зависит от контроля со стороны руководства за доступом работников, в т.ч. IT-специалистов, к компьютеру, с которого осуществляется доступ к системе ДБО.

2.11. Следует сменить пароль доступа к системе ДБО и принять повышенные меры по обеспечению отсутствия вредоносных программ (как минимум, проверить состояние антивирусного ПО и актуальность антивирусных баз, а также осуществить полную антивирусную проверку компьютера) в следующих случаях:

- При увольнении штатного IT-специалиста (системного администратора), осуществлявшего обслуживание компьютера, используемого для работы с системой ДБО.

- После любых действий внештатных IT-специалистов или любых других сотрудников, выполнявших любые операции на компьютере, используемом для работы с системой ДБО (например, решение каких-либо проблем, подключение к сети Интернет, установка,

обновление и поддержке различных бухгалтерских, правовых, информационных и др. программ и т.п.).

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

• сотрудниками организаций, в том числе уволенными, имеющими или имевшими доступ к носителям ключей ЭЦП (дискетам, флеш-дискам, жестким/сетевым дискам и пр.), а также доступ к компьютерам, с которых осуществляется работа с системой ДБО;

• IT-специалистами (штатными и внештатными), оказывающими (или оказывавшими ранее, в т.ч. однократно) различные IT-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, путём заражения компьютеров различными вирусами и вредоносным ПО (используя «бреши» в безопасности компьютеров и корпоративной сети организации), с последующим хищением через Интернет ключей ЭЦП и Средств Доступа к системе ДБО.

Во всех перечисленных случаях мошенники, завладев ключами ЭЦП и Средствами Доступа к системе ДБО Клиента, направляют от его имени в Банк платежи в адрес различных физических и юридических лиц.

3. Меры безопасности при использовании услуги «SMS авторизация».

3.1. SMS авторизация является средством дополнительной защиты доступа в «Интернет-Банк», в дополнении к логину и паролю, а также комплекту ЭЦП. Только получив одноразовый код доступа в виде SMS сообщения Вы сможете осуществлять расходные операции по Вашему расчетному счету через систему «Интернет-Банк»;

3.2. При использовании услуги «SMS авторизация» клиентам сервиса «Интернет-Банк» необходимо придерживаться следующих мер безопасности:

• не передавать телефон или SIM-карту в пользование третьим лицам;

• не пытаться войти в систему в местах, где полученное СМС с кодом аутентификации может быть подсмотрено третьими лицами;

• использовать разные SIM-карты и телефоны, если у Клиента зарегистрировано два и более лиц в системе «Интернет-Клиент».

незамедлительно обратитесь в Банк, в следующих случаях:

• если Вы потеряли телефон или SIM-карту;

• получили одноразовый SMS код для входа в систему, если Вы не пытались зайти в «Интернет-Банк»;

• одновременно получили большое количество одноразовых SMS сообщений от Банка.

Любой из вышеперечисленных случаев может быть признаком попытки мошеннического вывода денежных средства с Ваших счетов.

Обращаем Ваше внимание на то, что:

- АО КБ «КОСМОС» не осуществляет рассылку электронных писем с просьбой прислать ключи ЭЦП и/или пароль к системе ДБО и никогда не запрашивает у Вас эту информацию.

- Рассылка программ (или ссылок на них) по электронной почте для установки на Вашем компьютере может осуществляться только службой поддержки клиентов и систем ДБО Банка и только по предварительной договоренности с Вами.

В случае если Вы получили подобное «сомнительное» письмо от имени нашего Банка, содержащее программу для установки или запрос на предоставление ключей ЭЦП/паролей, используемых в системе ДБО, Вам следует незамедлительно сообщить об этом в службу технической поддержки клиентов и систем ДБО Банка.

После того, как Банк передал Вам Средства Доступа к системе ДБО (логин / пароль) и ключи ЭЦП, конфиденциальность полученных данных, а, следовательно сохранность Ваших денег, полностью зависит от того, насколько ответственно Вы отнесётесь к работе с системой ДБО.

Техническая поддержка Клиентов Банка по вопросам работы систем ДБО осуществляется по будням с 09.00 до 18.00.

Тел.: (495) 792-88-92