РЕКОМЕНДАЦИИ КЛИЕНТАМ БАНКА

по соблюдению мер информационной безопасности при использовании системы обмена электронными документами

(для размещения на сайте Банка)

1. Общие положения

1.1. Задачи защиты информации сводятся к минимизации ущерба и предотвращению воздействий со стороны злоумышленников. Для обеспечения надлежащей степени защищенности должен быть обеспечен комплексный подход, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне Банка, так и на стороне клиента.

1.2. Наиболее опасным является кража учетных данных – хищение личных данных клиента Банка и их незаконное использование для выполнения несанкционированных операций от имени клиента. Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций.

1.3. Риски получения несанкционированного доступа к информации прежде всего связаны с «фишингом» (использованием ложных ресурсов сети Интернет с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами), а также воздействием вредоносного кода.

1.4. «Фишинг» – попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

1.5. Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах, с которых осуществляется работа с системой, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее – ПО) либо на перехват информации, в том числе паролей.

1.6. Средства и методы защиты информации, применяемые в Банке, позволяют обеспечить необходимый уровень безопасности при осуществлении переводов денежных средств и предотвратить мошеннический вывод денежных средств со счетов клиентов при условии выполнения клиентами рекомендаций, изложенных в данном документе.

2. Рекомендации по защите информации от воздействия вредоносного кода.

2.1. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

2.2. Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.

2.3. Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).

2.4. Не используйте права администратора при отсутствии необходимости; в повседневной практике входите в систему с учетной записью пользователя, не имеющего прав администратора.

2.5. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ; старайтесь периодически просматривать журнал и реагировать на ошибки.

2.6. Не используйте на устройстве, предназначенного для доступа к системе ДБО, средства удаленного администрирования.

2.7. Обязательно установите и своевременно обновляйте на компьютере антивирусное программное обеспечение. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов пользователя при обнаружении вирусов. Лечение (удаление) зараженных файлов производится антивирусным средством в автоматическом режиме.

2.8. Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного средства.
2.9. Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы.
2.10. Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.
2.11. При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам Сети Интернет.
2.12. При работе в Интернет не соглашайтесь на установку каких-либо сомнительных программ.
2.13. Воздерживайтесь от использования программ онлайнового общения на компьютере, использующемся для работы в системе дистанционного банковского обслуживания.
2.14. Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ.
2.15. Рекомендуем ограничить информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты. Старайтесь не использовать компьютер, с которого Вы осуществляете переводы денежных средств, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.
2.16. Важно знать, что надежным средством обеспечения подлинности является цифровая подпись, а не строка адреса браузера или электронной почты. Часто в виде «интересной ссылки» в письме от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.
2.17. При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), полностью воздержаться от использования систем дистанционного банковского обслуживания и проведения платежей до исправления ситуации.
2.18. **Помните**, что Банк не несет ответственности в случае возникновения финансовых потерь, понесенных Клиентом в связи с нарушением и/или ненадлежащим исполнением им требований по защите от вредоносного кода своих автоматизированных рабочих мест (компьютера, ноутбука) для доступа к системе ДБО.

3. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

3.1. Мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете (например, Банка), и предназначены для сбора конфиденциальной информации обманным путем.

3.2. Злоумышленниками возможно создание фальсифицированных WEB-сайтов – их доменные имена и стили оформления могут имитировать сайты Банка и содержать ложные банковские реквизиты и контактную информацию. Вступление в какие- либо деловые отношения с лицами, представляющими ложный банк и использование подобных реквизитов, рискованно и может привести к нежелательным последствиям. Ввод логина и пароля на таком сайте приводит к получению этих данных злоумышленниками, т.е. разглашению идентификационных данных. Помните, что сайты, визуально напоминающие сайт СДБО, создаются специально для незаконного получения информации. В случае обнаружения фальсифицированного сайта, копирующего дизайн официального сайта или ДБО, пожалуйста, незамедлительно сообщите об этом по контактным телефонам Банка.

3.3. Во избежание использования ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемой Банком в системе ДБО, и (или) использующих зарегистрированные товарные знаки и наименование Банка, необходимо удостовериться, чтобы при подключении к СДБО защищённое SSL-соединение было установлено исключительно с официальным сайтом ДБО. Прежде чем ввести логин и пароль, Клиентам необходимо проверить по информации из SSL-сертификата подлинность сайта. Работу с ДБО рекомендуется осуществлять с использованием технических средств с индивидуальными дистанционно распознаваемыми идентификационными признаками (IPи MAC-адреса), предоставленными в Банк;

3.4. Перед просмотром электронного письма всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании. Изменить адрес электронной почты отправителя очень просто, поэтому будьте бдительны.

3.5. Внимательно читайте текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это – электронное письмо, отправленное мошенниками.

3.6. Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. В настоящем электронном письме Банк всегда приветствует Вас, обращаясь по имени и фамилии либо по названию компании. Типичное фишинговое письмо начинается с обезличенного приветствия.

3.7. Старайтесь сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Вас действовать быстро и необдуманно. Многие поддельные сообщения электронной почты пытаются убедить Вас в том, что Вашему счету угрожает опасность, если Вы немедленно не обновите критически важные данные.

3.8. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не переходите по этой ссылке.

4. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

4.1. Рекомендуется выделить отдельный компьютер, который использовать только для работы в системе ДБО (системе).

4.2. Рекомендуется регулярно менять пароль для работы со своими учетными данными в системе. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

4.3. Используемые в ДБО логин и пароль, запрещается записывать и хранить в местах, доступных посторонним лицам.

4.4. Необходимо хранить пароль в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования. Не рекомендуется записывать логин и пароль к ДБО там, где доступ к нему могут получить посторонние лица;

4.5. Генерацию рабочих ключей ЭП на E-token (Ключевом носителе) осуществляется владельцем ключа ЭП самостоятельно;

4.6. Использование Ключевого носителя должно осуществляться исключительно владельцем ключа ЭП . Рекомендуется хранить ключевую информацию на отчуждаемом носителе (USB-накопителе или дискете) и хранить его в сейфе или запираемом шкафу исключив возможность несанкционированного доступа.

4.7. Необходимо отключать, извлекать Ключевой носитель, если он не используются для работы в ДБО. Размещение Ключевого носителя в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключам ЭП третьими лицами;

4.8. Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные (например, сведения о Вашем банковском счете и т. д.).

4.9. В том случае, если Вы обнаружили, что Ваш пароль от банковской системы скомпрометирован, рекомендуем Вам незамедлительно сменить пароль на новый, известный только Вам, удовлетворяющий требованиям п. 4.1.

4.10. Если в процессе работы Вы столкнулись с тем, что ранее действующий пароль не срабатывает и не позволяет Вам войти в систему, необходимо как можно быстрее обратиться в Банк для получения инструкций по смене пароля.

4.11. Никому не разглашайте пароль от банковской системы. Банк не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные (в т.ч. пароли, PIN-коды и т.п.).

4.12. Не пересылайте файлы с конфиденциальной информацией для работы в банковской системе по электронной почте или через SMS-сообщения.

4.13. Рекомендуем исключить возможность физического доступа к компьютеру, с которого Вы осуществляете работу в системе персонала, не имеющего отношения к работе с ДБО и посторонних лиц.

4.14. Незамедлительно обращайтесь в Банк в том случае, если Вы получили уведомление системы об операции, которую Вы не проводили.

4.15. Размещение, охрана и специальное оборудование помещения, в котором установлены компьютеры, используемые для доступа в систему, должны обеспечивать сохранность информации, исключать возможность неконтролируемого проникновения в это помещение;

4.16. Принять меры по контролю конфигурации компьютера, с использованием которого осуществляется перевод денежных средств через ДБО, и её изменения. Не допускать несанкционированных программно-аппаратных изменений конфигурации;

4.17. На компьютере для работы с ДБО необходимо использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечить регулярную своевременную установку обновлений, выпускаемых разработчиками ДБО, операционной системы, web-браузеров (Microsoft Internet Explorer, Mozilla FireFox, Opera и т.д.) и иного прикладного программного обеспечения;

4.18. Применять на компьютере для работы с ДБО лицензионные средства антивирусной защиты, обеспечить регулярное автоматическое обновление компонентов антивирусной защиты;
4.19. Рекомендуется применять на компьютере для работы с ДБО специализированные программные и аппаратные средства безопасности: средства защиты от несанкционированного доступа, персональные межсетевые экраны, антишпионское программное обеспечение и т.п., обеспечить регулярное автоматическое обновление программного обеспечения этих средств;
4.20. На компьютере для работы с ДБО необходимо исключить посещение WEB- сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т.п. Использование нелицензионного программного обеспечения повышает риск получения несанкционированного доступа злоумышленников с целью хищения денежных средств;
4.21. Не допускается работать с ДБО на компьютерах в Интернет-кафе или на других компьютерах общего пользования (вокзалы, аэропорты, библиотеки и т.п.). Работа с гостевых рабочих мест увеличивает риск неправомерного использования ключа ЭП и другой аутентификационной информации;
4.22. Рекомендуется установить пароли на учётные записи пользователей операционной системы на компьютере для работы с ДБО. Работу с ДБО на компьютере осуществлять только под учетной записью с ограниченными правами в операционной системе. Не допускать штатную работу в ДБО под учетной записью с правами администратора в операционной системе компьютера;
4.23. В случае компрометации или подозрении на компрометацию закрытого ключа ЭП, для предотвращения несанкционированного доступа к управлению счетом, в том числе при утрате (потере, хищении) Ключевого носителя, с использованием которого Клиент осуществляет перевод денежных средств, Клиенту необходимо незамедлительно обратиться в Банк для блокирования скомпрометированных ключей ЭП;
4.24. Регулярно проводить контроль сумм и получателей электронных документов в информационном окне ДБО, а также контролировать количество и сумму отправленных электронных документов;
4.25. Регулярно контролировать состояние своих счетов и незамедлительно сообщать в Банк обо всех подозрительных или несанкционированных изменениях;
4.26. При обслуживании компьютера сотрудниками технической поддержки организации Клиента или сторонних организаций – обеспечивать контроль выполняемых ими действий;
4.27. Не передавать Ключевой носитель сотрудникам технической поддержки для проверки работы ДБО, проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только лично владелец ключа ЭП должен подключить Ключевой носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейсе ДБО, и лично ввести пароль, не допуская ознакомления с ним посторонних лиц;
4.28. В случае передачи (списания) компьютера, на котором ранее была установлена ДБО, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу организации Клиента, в том числе следы работы в ДБО;
4.29. При увольнении ответственного сотрудника, имевшего доступ к Ключевому носителю, уведомить Банк об увольнении и действовать в соответствии с Договором дистанционного банковского обслуживания с использованием электронных документов и электронной подписи.
4.30. Необходимо корректно завершать работу в ДБО, используя для этого пункт меню «Выйти из системы».

5. Рекомендации по безопасности при использовании мобильных устройств для доступа к дистанционному банковскому обслуживанию.

5.1. Не совмещайте устройства доступа к услуге «Мобильный банк» и устройства получения SMS-сообщений с подтверждающим одноразовым паролем (например, мобильный телефон, смартфон или планшет).

5.2. При утрате мобильного телефона, на который Вы получаете сообщения с SMS-паролем, сразу же обратитесь к оператору сотовой связи и заблокируйте SIM-карту.

5.3. При потере мобильного телефона с подключенным мобильным приложением следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты и в Банк для блокировки услуги «Мобильный банк»

5.4. При смене номера телефона, на который подключена услуга «Мобильный банк», необходимо отключить услугу «Мобильный банк» от старого номера телефона и подключить услугу на новый номер. Помните, что операторы сотовой связи могут передать номер телефона другому абоненту, если он будет неактивным длительное время.

5.5. Будьте внимательны — не оставляйте свой телефон без присмотра, чтобы исключить несанкционированное использование мобильных банковских услуг. Установите на телефоне пароль, данная возможность доступна для любых современных моделей телефонов/смартфонов.

5.6. Не подключайте к услуге «Мобильный банк» телефоны, которые Вам не принадлежат, по просьбе третьих лиц, даже если к Вам обратились от имени сотрудников Банка.

5.7. При установке на телефон дополнительных программ обращайте внимание на полномочия, которые необходимы программе. Если программе требуются излишние полномочия это повод проявить настороженность. Обращайте внимание на такие опасные разрешения: доступ и отправка SMS, доступ к Интернет.

5.8. Установите на телефон антивирусное ПО и своевременно его обновляйте.

5.9. При внезапном прекращении работы SIM-карты необходимо обратиться к оператору сотовой связи за уточнением причин — в отношении Вас возможно проведение мошеннических действий третьими лицами.

5.10. Не взламывайте телефон, так как это отключает защитные механизмы, заложенные производителем. В результате ваш телефон становится уязвимым к заражению вирусным ПО.