****

**РЕКОМЕНДАЦИИ**

**Клиенту по обеспечению безопасности при работе**

**с системой дистанционного банковского обслуживания Банк-Клиент через Интернет**

**1. Общие рекомендации**

Данные рекомендации состоят из наилучших практик обеспечения информационной безопасности и предотвращения мошенничества при использовании СКБ. Часть из рекомендаций может быть легко выполнена уверенным пользователем ПК. Для выполнения других рекомендаций Вам может потребоваться помощь / консультирование ваших сотрудников поставщиком услуг ИТ-поддержи, а также привлечение к данному вопросу лиц, ответственных за обеспечение информационной и экономической безопасности.

Активное развитие ИТ-технологий требует от руководителей компаний и лиц, осуществляющих работу в системе Банк-Клиент, знание и понимание современных угроз и способов предотвращения / минимизации последствий кибер-атак на организацию. Банк прилагает усилия для предотвращения мошенничества при использовании клиентами системы Банк-Клиент, но в случае, если клиенты не будут проявлять должную осмотрительность, будут игнорировать требования по обеспечению информационной и экономической безопасности, деньги организации могут быть похищены злоумышленниками.

Наиболее эффективным является обучение сотрудников на основе данных рекомендаций и других учебных материалов, которые доступны в сети Интернет. Если в Вашей организации количество сотрудников, работающих на ПК более 20 (двадцати) – хорошей практикой будет регулярное тестирование сотрудников на соблюдение правил информационной безопасности.

Рекомендуем поделиться данными требованиями с вашими контрагентами и лицами/компаниями, осуществляющими ИТ-поддержку и сопровождение вашей организации. Также, для поддержания необходимого уровня осведомленности об актуальных кибер-угрозах рекомендуем Вам и Вашим специалистам подписаться на новостные рассылки и регулярно просматривать сайты компаний, осуществляющих борьбу с кибер-преступностью (например, Лаборатория Касперского, Group-IB и др.)

Просим Вас при поступлении из Банка запросов о подтверждении той или иной операции проявлять необходимую бдительность и внимание при перепроверке и предоставлении дополнительной информации относительно реквизитов получателя и источника/способа их получения.

**1.1 Обеспечение безопасности компьютера, с использованием которого осуществляется работа в системе Банк-Клиент:**

**1.1.1** Перед входом в систему Банк-Клиент необходимо удостовериться в том, что на компьютере, с использованием которого осуществляется работа в системе Банк-Клиент, отсутствуют вредоносные программы, на компьютере установлено, активировано и работает современное лицензионное антивирусное программное обеспечение, антивирусные базы обновляются ежедневно. Только регулярные обновление антивирусных баз и проведение антивирусных проверок позволит Вам своевременно обнаружить и предотвратить появление вредоносных программ (особенно важно контролировать обновление, если нет постоянного подключения к Интернету).

**1.1.2** На компьютере рекомендуется использовать только лицензионное программное обеспечение, регулярно устанавливать рекомендуемые производителями обновления, как операционной системы, так и прикладного программного обеспечения, в том числе браузера, программ работы с документами (офис, просмотр файлов PDF), бухгалтерских программ. Все это позволит устранить выявленные в ПО уязвимости, которые могут быть использованы третьими лицами для получения несанкционированного доступа к компьютеру и к системе Банк-Клиент.

**1.1.3** Рекомендуется использовать на Вашем компьютере персональный межсетевой экран для входа в Интернет. Это позволит значительно снизить риск удаленного управления Вашим компьютером злоумышленниками из Интернет и локальной сети, а также может предотвратить кражу конфиденциальной информации. Дополнительно в настройках персонального межсетевого экрана рекомендуется разрешить подключение вашего Компьютера только к следующим ресурсам: сервер системы Банк-Клиент (<https://78.111.247.129> или https://78.111.247.129/ibank2/#/), серверам обновлений разработчиков используемого программного обеспечения, минимально необходимое количество соединений по конкретным портам доступа для осуществления обмена внутри офисной сети. Любые иные подключения рекомендуется запретить.

**1.1.4** При подготовке платежных документов на других компьютерах (документов, содержащих реквизиты для платежа) учитывайте, что подмена реквизитов может произойти на любом из компьютеров, где данная информация будет обрабатываться или передаваться.

**1.1.5** Рекомендуется осуществлять работу в системе Банк-Клиент с использованием отдельной учетной записи в операционной системе компьютера, защищенной сложным паролем, известным только Вам. При возможности рекомендуется осуществлять доступ в систему Банк-Клиент с выделенного компьютера, используемого исключительно для работы с системой Банк-Клиент. Права пользователя в операционной системе компьютера должны быть минимально необходимыми, должна быть запрещена установка прикладного программного обеспечения за исключением необходимого для работы в системе Банк-Клиент.

**1.1.6** Рекомендуется избегать работы в системе Банк-Клиент с «недоверенных» компьютеров (в Интернет-кафе или с других общедоступных компьютеров, а так же с «чужих» компьютеров, временно используемых Вами и т.п.). Крайне нежелательно использовать для работы в системе Банк-Клиент публичные беспроводные сети (например, бесплатный Wi-Fi и т.п.), вместо этого лучше воспользоваться «мобильным Интернетом» (LTE/GPRS/EDGE/HSPA/3G соединение). При использовании компьютеров и сетей доступа, не контролируемых Вами, существенно возрастает риск компрометации Ваших учетных данных, кражи денежных средств и конфиденциальных данных т.к. злоумышленники /другие пользователи могли установить/заразить вредоносным ПО данное оборудование. В случае, если вы по каким-либо причинам не смогли выполнить данную рекомендацию, постарайтесь в кратчайшие сроки подключится к системе Банк-Клиент с доверенного устройства из надежной сети и измените пароль доступа на новый.

**1.1.7** Не оставляйте без присмотра компьютер с активной сессией системы Банк-Клиент.

**1.1.8** Использование компьютера, на котором производится подготовка, обработка и отправка платежных документов, для просмотра сайтов (как с деловым содержанием, так и потенциально опасных Интернет-ресурсов - социальные сети, форумы, чаты, телефонные сервисы и т.п.), работы с внутренней или внешней электронной почтой, в которой могут содержаться вложения или ссылки для загрузки вредоносного ПО, может привести к заражению компьютера и краже денежных средств в системе Банк-Клиент или к подмене реквизитов платежных документов при их загрузке/вводе.

По возможности исключите посещение с данного компьютера сайтов сомнительного содержания и любых других потенциально опасных Интернет-ресурсов, а также чтение почты и открытие почтовых документов. Помните, что почтовый документ, полученный от Вашего контрагента, известной компании или государственной службы, может быть результатом работы злоумышленников по имитации настоящего документа или мог быть отправлен в результате вирусного заражения компьютера отправителя сообщения, в том числе и Вашего контрагента.

**1.1.9** В случае использования в компании собственного почтового сервера, необходимо убедиться, что используемое решение поддерживает функционал анализа содержимого почтовых сообщений не только на вирусы, но и обнаруживает в безопасной среде («песочница») аномальное поведение вложений и файлов, которые могут загружаться по ссылкам из сообщений. Решения класса «песочница» не обязательно покупать и устанавливать в организации – они могут быть уже встроены в сервисы электронной почты, предоставляемые крупными провайдерами, или могут быть арендованы в виде облачного решения.

**1.1.10** Если вам был передан USB-накопитель (флешка) или вы получили по электронной почте заархивированные с паролем файлы или файлы офисных форматов doc, docx, xls, xlsx, ppt, pptx; файлы, содержащие макросы docm, xlsm, pptm, а также файлы Adobe Acrobat формата PDF, для открытия которых необходимо ввести пароль – помните, что такие файлы не могут быть проверены средствами обнаружения вредоносного ПО (антивирус или песочница), поэтому представляют высокий риск для заражения компьютера. Не используйте такие файлы на компьютере, с которого осуществляется доступ в систему Банк-Клиент. Если вам нужны такие файлы – работайте с ними на других компьютерах, предварительно убедившись, что файл получен из надежного источника, и пароль был установлен именно его отправителем. Если файл в архиве, его необходимо извлечь из архива и проверить антивирусным ПО.

**1.1.11** Очень часто злоумышленники для получения удаленного доступа в сеть компании используют различные тактики социальной инженерии. Одна из таких схем – попытка узнать у пользователей их учетные записи (логин) и пароль по телефону или с помощью различных сообщений, поддельных страниц банка в сети Интернет. Еще одним вариантом проникновения в сеть компании является схема, когда возле офиса компании подбрасывается USB-носитель (флешка), на которой может быть нанесена маркировка/логотип компании или какой-либо другой логотип, который может заинтересовать сотрудников и побудить их попытаться открыть содержимое носителя на рабочем компьютере. В результате открытия такого носителя компьютер может оказаться под удаленным управлением злоумышленника.

**1.2 Правила безопасности при работе в системе Банк-Клиент.**

**1.2.1** Перед вводом логина и пароля при входе в систему Банк-Клиент убедитесь, что соединение установлено именно со стартовой страницей системы Банк-Клиент и в адресной строке web-браузера отображается <https://78.111.247> (или https://78.111.247.129/ibank2/#/). Злоумышленники могут создать мошеннический ресурс с похожим адресом системы Банк-Клиент. Если Вы заметили, что адрес отличается или есть иные причины вызывающие подозрения в подлинности адреса (например, сообщение web-браузера о перенаправлении на другой сайт), то не вводите никакой конфиденциальной информации и незамедлительно сообщите о данном факте в Банк по телефону техподдержки.

**1.2.2** При работе с системой Банк-Клиент для обеспечения конфиденциальности весь трафик между Банком и вашим компьютером шифруется с помощью защищенного протокола TLS (Transport Layer Security). Перед началом работы в системе Банк-Клиент необходимо удостовериться, что соединение установлено в защищенном режиме TLS. В префиксе в адресной строке web-браузера должен появиться символ S - https://78.111.247.

**1.2.3** После окончания работы в системе Банк-Клиент обязательно завершайте сеанс работы.

**1.3 Соблюдайте правила безопасности при работе с ключевыми носителями:**

**1.3.1** Уделите вопросу хранения ключей должное внимание. Помните, что наличие ключа позволяет заверить от Вашего имени документ и передать его на исполнение в Банк. Для большей безопасности храните ключи на съемных защищенных ключевых носителях (Рутокен ЭЦП 2.0., eToken, iKey1000).

**1.3.2** Подключайте ключевой носитель к компьютеру только на время подписи документов. Не держите ключевые носители постоянно подключенными к компьютеру. Ни в коем случае не храните ключи на жестком диске компьютера.

**1.3.3** Постарайтесь внедрить использование для отправки документов двух подписей (2-х ключей).

Осуществляйте подпись документов 1-й и 2-й подписями с различных компьютеров. Украсть два ключа сложнее, чем один.

**1.3.4** При вводе ключа и пароля особое внимание, обращайте на правильное отображение названия ключа.

**1.3.5** При компрометации секретных ключей или компьютера, увольнения ответственного сотрудника или ИТ специалиста Вашей компании, который имел доступ к компьютеру или к секретным ключам незамедлительно сообщите в Банк для блокировки ключей и генерации новых.

**1.4 Соблюдайте правила безопасности при использовании паролей**

**1.4.1** Для работы в системе Банк-Клиент необходимо использовать только сложные пароли, удовлетворяющие следующим требованиям:

− пароль должен иметь длину от 6 до 20 символов, в нем должно быть не менее двух цифр и двух букв, допускается использование букв латинского алфавита, цифр, знаков !#$%&()\*+- ./:;<=>?[\;

− пароль не должен содержать последовательности одинаковых символов и групп символов, легко угадываемые комбинации символов (dddddd, 333444555, qwerty, 12345, abc123 и т.п.);

− пароль не должен содержать связанных c Вами данных (имена и даты рождения членов семьи, адреса, телефоны, часть номера вашей банковской карты и т.п.);

− пароль не должен содержать словарных слов (passw0rd, football, shadow, sergey, natalia, русские слова, набранные в английской кодировке, например, Сергей – Cthutq);

− пароль не должен совпадать с предыдущими паролями и не должен совпадать с именем входа;

− пароль не должен быть копией или комбинаций паролей используемых Вами в других системах (операционная система компьютера, электронная почта, развлекательные ресурсы в Интернет и т.п.).

**1.4.2** Никогда не сообщайте свой пароль третьим лицам, в том числе коллегам, родственникам и сотрудникам Банка, вводите пароль только при работе в системе Банк-Клиент. Сотрудник Банка не имеет права запрашивать у Вас пароль, даже если вы самостоятельно обратились в Банк. Вводите пароль только в системе Банк-Клиент. Банк никогда не отправляет сообщений по электронной почте или SMS-сообщений с просьбой уточнить или предоставить пароль.

**1.4.3** Не записывайте свой пароль там, где доступ к нему могут получить третьи лица. Запрещается сохранять пароль на компьютере, мобильном устройстве, а также на иных электронных носителях, доступ к которым могут получить третьи лица.

**1.4.4** Рекомендуется осуществлять смену пароля доступа к системе Банк-Клиент не реже одного раза в 3 месяца.

**1.4.5** При возникновении подозрений, что Ваш пароль стал известен третьим лицам, необходимо незамедлительно сменить пароль или заблокировать доступ в систему Банк-Клиент, обратившись в Банк по телефону техподдержки.

**В случае утраты, а также при возникновении любых подозрений, что Ваши логин и пароль стали известны третьим лицам (в том числе представившимся сотрудниками Банка), незамедлительно предпринимайте меры для блокировки системы Банк-Клиент. Вы можете сделать это, связавшись с Банком по телефону техподдержки.**

**1.4.6.** При использовании внешних сервисов электронной почты используйте сервисы, предоставляющие двухфакторную аутентификацию (ввод одноразового пароля, сгенерированного специальным приложением). Это позволит защитить направляемую на Ваш почтовый ящик информацию от доступа третьих лиц.

**1.5 Рекомендации по предотвращению мошенничества:**

**1.5.1** Контролируйте в системе Банк-Клиент реквизиты получателя при подписи и отправке в Банк ЭД, импортированных из внешних систем (1С, Мое Дело и др.) Зафиксированы случаи подмены реквизитов получателей вредоносным ПО в процессе импорта в системе Банк-Клиент.

**1.5.2** Сверяйте с контрагентами по телефону реквизиты на оплату при получении новых реквизитов дистанционно (по электронной почте, курьером и т.п.). Для сверки реквизитов запрещено использовать контактные данные, указанные в подозрительном письме, т.к. они также могут принадлежать мошенникам. Необходимо использовать контактные данные контрагента, которые использовались ранее, или проверить информацию на официальном интернет-сайте контрагента.

Фиксируются случаи, когда злоумышленники встраиваются в общение между контрагентом и заказчиком, и им удается от имени контрагента направить реквизиты «подставной» компании, через которую денежные средства похищаются. Для этого злоумышленники используют современные средства коммуникации – электронную почту контрагента, к которой они смогли получить доступ, или почтовый ящик на бесплатном сервисе, оформленный и похожий на настоящий адрес контрагента, мессенджеры.

**1.5.3** Проводите дополнительную проверку компании контрагента. Введя ИНН организации на поисковом сайте в Интернет можно, используя бесплатные сервисы, узнать об организации: дату регистрации, ФИО генерального директора / учредителя, вид деятельности, а также были ли изменения в ее руководстве. Для кражи денежных средств злоумышленники обычно используют либо компании, которые были недавно зарегистрированы на подставных лиц, либо юридические лица, которые были приобретены у предыдущих владельцев вместе с расчетным счетом, системой Банк-Клиент и пластиковыми картами для быстрого снятия похищенных денежных средств. Во втором случае в информации о компании может отображаться дата внесения изменений в регистрационные данные компании.

Если у вашей организации нет ресурсов для поиска информации о контрагенте в Интернет, информацию о контрагенте вы можете получить в рамках сервиса «Проверка контрагентов», предоставляемой Банком.

**1.5.4** Банк никогда не связывается по телефону и не осуществляет рассылок сообщений по SMS или e-mail с просьбой предоставить, подтвердить или уточнить Вашу конфиденциальную информацию (пароли, логины, кодовое слово, Ф.И.О., паспортные данные, номер мобильного телефона, на который приходят одноразовые пароли и другие конфиденциальные данные). Не отвечайте на такие сообщения.

**1.5.5** Банк никогда не связывается с просьбой установить или обновить программное обеспечение, в своих электронных письмах никогда не рассылает программы. Не открывайте подозрительные файлы, присланные вам по электронной почте. Файлы в форматах, указанных в пункте 1.1.10, могут содержать вредоносное ПО.

**1.5.6** При получении подозрительного сообщения от имени Банка не отвечайте на него, не переходите по ссылкам, указанным в подозрительном сообщении (даже если адрес похож на адрес официального Интернет-сайта Банка). Банк не направляет сообщения с просьбой осуществить вход в систему Банк-Клиент по указанной в сообщении ссылке.

**1.5.7** При работе с системой Банк-Клиент обратите внимание на страницу входа и интерфейс, если вы заметите любые отличия, не заявленные ранее Банком, или возникнут иные причины для возникновения подозрений в том что ресурс поддельный, необходимо незамедлительно прекратить работу и обратиться в Банк по телефону техподдержки (никогда не связывайтесь по телефону указанному на подозрительной странице).

**1.5.8** Если вы самостоятельно связались с Банком, сотрудники могут уточнить у Вас персональную информацию, но не имеют права запрашивать у Вас пароль на вход в систему Банк-Клиент.

**1.5.9** Сотрудники Банка никогда не связываются по телефону, чтобы сообщить о недоступности системы Банк-Клиент вследствие проведения регламентных работ. Если Вы получили подозрительное сообщение от имени Банка либо с Вами связались по телефону с одной из просьб, перечисленных в данном разделе, то рекомендуется сообщить о данном факте в Банк по телефону техподдержки (никогда не связывайтесь с Банком по телефону, указанному в подозрительном сообщении).

**1.5.10** Обращайте внимание на появление подозрительной активности на Вашем компьютере, например, самопроизвольные движение курсора на экране, набор текста и т.п. Обращайте внимание на невозможность осуществить вход в систему Банк-Клиент при том, что другие Интернет-сайты у Вас загружаются, а так же на невозможность войти в систему Банк-Клиент по причине несовпадения логина и пароля, притом, что они корректны. Обращайте внимание на «зависания» системы Банк-Клиент при нормальной работе других Интернет-сайтов. Данные факты могут свидетельствовать о заражении Вашего компьютера вредоносными программами. Избегайте работы в системе Банк-Клиент с зараженных компьютеров, если на зараженном компьютере уже осуществлялась работа в системе Банк-Клиент, то незамедлительно заблокируйте Вашу учетную запись в системе Банк-Клиент. Вы можете сделать это, связавшись с Банком по телефону техподдержки.

**1.5.11** В случае если, по Вашему мнению, произошло несанкционированное списание денежных средств, необходимо незамедлительно обратиться в Банк с сообщением о несанкционированном списании.

В случае если операция не совершалась ни Клиентом, ни его представителем, а так же имеются иные признаки незаконного завладения денежными средствами (кражи) с использованием системы Банк-Клиент, то после обращения в Банк Вам рекомендуется оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (глава 21 УК РФ). После чего предоставить в Банк копию заявления о возбуждении уголовного дела, либо копию талона-уведомления, подтверждающего непосредственное обращение в правоохранительные органы и содержащего порядковый номер из книги учета сообщений о преступлениях содержащую отметку правоохранительного органа о его приеме.

**Помните, что Ваше оперативное обращение в Банк может предотвратить несанкционированное списание, либо приостановить списание денежных средств, снизив Ваши финансовые потери.**

**1.6 Правила поведения в случае, если произошел инцидент информационной безопасности:**

**1.6.1** Если с помощью антивирусного ПО Вы обнаружили на компьютере, где используется система Банк-Клиент, или на любом другом компьютере, который используется для обработки платежных документов, вирус, необходимо:

**1.6.1.1** Отключить компьютер от телекоммуникационной сети (Интернет), вытащив из компьютера сетевой кабель или отключив WiFi соединение.

**1.6.1.2** Осуществить поиск в интернет по названию вируса, чтобы понять – может ли данный вирус использоваться как банковский троян, вирус для подмены реквизитов или для осуществления удаленного управления компьютером.

**1.6.1.3** Если вирус соответствует указанным выше категориям, Вам необходимо с другого компьютера направить в Банк сообщение о вирусном заражении и возможном хищении денежных средств.

**1.6.1.4** Не производите лечение файлов с помощью антивирусного ПО и не удаляйте какую-либо информацию с зараженного компьютера. В случае кражи денежных средств Вам могут

потребоваться цифровые улики, оставленные злоумышленниками.

**1.6.1.5** После обращения в Банк следуйте полученным инструкциям.

**1.7 Другие вопросы:**

**1.7.1** При использовании услуг ИТ-поддержки, предоставляемых контрагентом или частными лицами, убедитесь, что они внимательно ознакомились с данными рекомендациями. Если у них возникли какие-либо вопросы по реализации данных требований – Вы можете направить вопросы в службу поддержки Банка.

Поделитесь данными рекомендациями с вашими контрагентами, т.к. одной из причин отправки денежных средств на счет мошенников может быть подмена реквизитов на стороне контрагента – еще до того, как вы получили от них счет на оплату.

**2. При эксплуатации средств защиты информации (Настоящие рекомендации определяются условиями лицензирования ФСБ деятельности Банка, а также требованиями ФСБ к средствам криптографической защиты конфиденциальной информации).**

**2.2** Рекомендации по организационному обеспечению безопасности средств защиты информации (далее - СЗИ):

− в организации Клиента выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СЗИ;

− в организации Клиента разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СЗИ;

− к работе с СЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СЗИ.

**2.3** Рекомендации по размещению СЗИ и режиму охраны:

− помещения, в которых размещаются технические средства клиентского рабочего места со встроенными СЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ;

− размещение режимных помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств;

− размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности;

− входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время;

− окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией;

− размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна;

− в режимные помещения допускаются руководители организации Клиента, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов;

− системные блоки компьютеров с СЗИ оборудуются средствами контроля вскрытия;

− ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СЗИ.

**2.4** Рекомендации по обеспечению безопасности ключевой информации:

− необходимо по возможности производить резервное копирование рабочих ключевых носителей с ключами АСП;

− ключевые носители в организации Клиента берутся на поэкземплярный учет в выделенных для этих целей журналах;

− учет и хранение ключей поручается руководством Клиента специально выделенным сотрудникам;

− для хранения ключевых носителей с ключами АСП выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации;

− хранение ключей допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное применение, не предусмотренное правилами пользования СЗИ;

− ключевые носители с рабочими ключами (копиями рабочих ключей) хранятся раздельно с обеспечением условия невозможности их одновременной компрометации;

− при транспортировке ключевых носителей с секретной ключевой информацией создаются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

Ознакомлен: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (наименование организации/ФИО) (подпись)

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 \_\_\_\_г.