**РЕКОМЕНДАЦИИ КЛИЕНТАМ БАНКА**

**по соблюдению мер информационной безопасности при работе с системой дистанционного банковского обслуживания «Клиент-Банк» (для клиентов юридических лиц Эс-Би-Ай Банк ООО)**

**Уважаемые Клиенты!**

Соблюдение приведенных рекомендаций позволит максимально безопасно работать с системой дистанционного банковского обслуживания «Клиент-Банк» (далее, Система ДБО), минимизировать риски информационной безопасности и электронного мошенничества, а также обеспечить сохранность денежных средств, размещенных на Ваших счетах:

1. **Для работы с Системой ДБО необходимо использовать отдельную рабочую станцию (или ноутбук), доступ к которой имеют только лица, осуществляющие платежи в Системе ДБО, и удовлетворяющее следующим требованиям:**
   - использовать лицензионную и поддерживаемую производителем версию операционной системы с регулярным автоматическим обновлением безопасности (например, ОС Windows XP уже не поддерживается с 2014 года, поддержка Windows 7 заканчивается 14 января 2020 года);
     ограничить права пользователей с целью исключения возможности несанкционированного изменения конфигурации операционной системы или установки программного обеспечения; исключить использование учетных записей с правами администратора;
   - обеспечить наличие лицензионных средств защиты от вредоносного программного обеспечения с автоматическим обновлением антивирусного продукта и сигнатурных баз (например, Kaspersky , Dr. Web, Symantec, Avira, ESET, McAfee); средства защиты от вредоносного программного обеспечения должны запускаться автоматически, с загрузкой операционной системы; по умолчанию рекомендуется установить максимальный уровень политик безопасности средств защиты от вредоносного программного обеспечения, т.е. не требующих ответов пользователя при обнаружении вредоносного ПО;
   - организовать проведение регулярного полного сканирования рабочего места (не реже одного раза в неделю) средствами защиты от вредоносного программного обеспечения на предмет наличия вирусов и вредоносного программного кода; проверку осуществлять согласно расписанию, которое можно выставить в настройках средства защиты от вредоносного программного обеспечения;
   - средства защиты от вредоносного программного обеспечения должны быть настроены на проведение обязательного контроля любой информации, получаемой и передаваемой по телекоммуникационным каналам, а также информации на съемных носителях (CD/DVD дисках, USB-накопителях (флешки) и т.п.); настроить возможность сканирования в автоматическом режиме;
   - рекомендуется установка и настройка межсетевого экрана (допускается использование встроенного межсетевого экрана в средства защиты от вредоносного программного обеспечения) для защиты локальной сети организации от внешних вторжений и/или использование настроенного персонального межсетевого экрана на рабочее место, с которого осуществляется вход в Систему ДБО; ограничение доступа на уровне сети существенным образом снижает вероятность несанкционированного доступа к рабочей станции (ноутбуку) из сети Интернет;

- рекомендуется организовать периодическую проверку контроля целостности файлов операционной системы, а также сертифицированных средств криптографической защиты информации;
- не рекомендуется использовать рабочее место для посещения сайтов сети Интернет, отличных от сайта Системы ДБО; в случае использования сети Интернет или почты, исключить посещение незнакомых сайтов, не загружать ничего из сети на данную рабочую станцию (ноутбук), не открывать на нем вложения в электронные письма и электронные письма от неизвестных отправителей;
- Обеспечить выполнение правил пользования СКЗИ, размещенных на официальном сайте банка на странице https://ibank.sbibankllc.ru/docs/Corporate_Internet-Banking_WEB_ShortGuide.pdf в разделе «Требования».

2. **Рекомендации по защите от несанкционированного доступа со стороны третьих лиц (то есть лиц, неуполномоченных Клиентом на работу с Системой ДБО):**

- рекомендуется настройка автоматической блокировки экрана при отсутствии за рабочей станцией более 10 минут;
- отключение в настройках операционной системы кеширования паролей;
- регулярная смена паролей для работы со своими учетными записями в системе; соблюдение к требованию уникальности и сложности пароля: длина пароля должна содержать не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов;
- используемые логин, пароль и блокировочное слово необходимо хранить в тайне и предпринимать необходимые меры предосторожности для предотвращения их несанкционированного использования; не сохранять пароли и блокировочные слова в электронном виде или на бумажных носителях; не разглашать пароль от банковской системы даже работникам Банка;
- не допускать третьих лиц к электронным носителям информации и электронным устройствам, на которых установлено программное обеспечение системы, или которые используются при работе с системой, а также сотовым телефонам, используемым для услуги SMS-подтверждения платежей;
- в случае подозрения на компрометацию пароля от банковской системы, рекомендуется незамедлительная его смена и направление информации в Банк о компрометации;
- размещение, охрана и специальное оборудование помещения, в котором установлена рабочая станция (ноутбук), используемые для доступа в Систему ДБО, должны обеспечивать сохранность информации, исключать возможность неконтролируемого проникновения в это помещение;
- незамедлительно обращайтесь в Банк в том случае, если Вы получили уведомление Системы ДБО об операции, которую Вы не проводили;
- при проведении платежей сверяйте сумму перевода, отраженную на экране монитора с информацией в SMS-сообщений, а также контролируйте количество и сумму отправленных электронных документов; при обнаружении расхождений между данными системы и фактически выполненными платежами, немедленно информируйте об этом Банк;
- регулярно контролировать состояние своих счетов и незамедлительно сообщать в Банк обо всех подозрительных или несанкционированных изменениях;
- **Категорически запрещено:** 1) посещать социальные сети (например, ВКонтакте, Одноклассники, Facebook и др.), и другие ресурсы, не связанные с должностными обязанностями работника Организации; 2) устанавливать и

использовать программы мгновенного обмена сообщениями (например, ICQ, QIP, Mail.ru agent, Miranda); 3) устанавливать и использовать ПО для облачного хранения данных (например, GoogleDisk, YandexDisk, DropBox, Mail cloud и др.); 4) устанавливать и использовать программы, обеспечивающие голосовую и видео связь (Skype, Viber, Microsoft Lync и т.п.); ВАЖНО: Возможность подключения к личным почтовым ящикам, интернетсистемам обмена экспресс-сообщениями, а также сайтам социальных сетей должна быть исключена; 5) устанавливать, запускать, использовать на рабочей станции (ноутбуке) программного обеспечения для удаленного управления (например, RDP, TeamViewer, Radmin, Ammyy Admin др.).

3. **Обеспечение идентификации, авторизации клиентов и подтверждение подлинности платежных документов в Системе ДБО:**
    - в целях обеспечения идентификации, аутентификации, подтверждения подлинности платежных документов в Системе ДБО используется система криптографической защиты информации (СКЗИ) сертифицированная по требованиям безопасности ФСБ России;
    - при работе с СКЗИ и электронной подписью необходимо сохранять в тайне пароль к ключу электронной подписи, в качестве места хранения носителя использовать персональный сейф;
    - запрещается записывать на носители ключевой информации постороннюю информацию, передавать носитель с ключевой информацией другим лицам и разглашать пароль к ключу электронной подписи;
    - запрещается оставлять подключенным к компьютеру носитель ключа электронной подписи дольше, чем это необходимо для работы с системой удаленного банковского обслуживания;
    - запрещается снимать несанкционированные копии с носителей ключевой информации;
    - необходимо производить замену ключей электронной подписи до истечения срока их действия;
    - производить внеплановую замену ключей электронной подписи в случаях увольнения и смены лиц, имеющих доступ к Системе ДБО, в том числе IT-специалистов, а также руководителей с правом подписи доверенностей на получение электронной подписи, и в случае подозрений на компрометацию ключа электронной подписи;
    - не осуществляйте вход в систему в местах, где услуги подключения к сети Интернет являются общедоступными, например, в Интернет-кафе;

4. **Служба поддержки Банка**
    - 8(495) 651-65-12 (для Москвы и Московской области)
    - 8(800) 700-65-12 (по России, звонок бесплатный, круглосуточно)

5. **Действия Клиента при обнаружении факта доступа постороннего лица к Системе/к устройствам, используемым для работы в Системе ДБО**:
    - немедленно прекратить любые действия с электронными устройствами: компьютер, ноутбук и т.п., подключенным к Системе ДБО, обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь аккумуляторную батарею из ноутбука и т.п.) и отключить от информационных сетей;
    - при наличии технической возможности отозвать перевод с использованием иного электронного устройства, после чего заблокировать Систему ДБО и немедленно обратиться в Банк;
    - при отсутствии технической возможности отозвать перевод по Системе ДБО, немедленно обратиться в Банк по телефону 8(495)000-00-00 с заявлением о приостановке исполнения платежа и возврате средств.

- проинформировать все банки, с которыми клиент имеет договорные отношения, предусматривающие использование Системы ДБО, установленными на рабочем месте и обратиться с просьбой о внеплановой замене ключевой информации.
- обратиться в банк плательщика с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к Системе ДБО, а также о компрометации ключей и необходимости смены пароля (закрытого ключа). Копия заявления должна быть направлена в банк плательщика незамедлительно по электронной почте. Оригинал заявления должен быть доставлен в банк плательщика курьером или по почте.
- оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (глава 21 УК РФ). Копию заявления предоставить в Банк.
- Оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить копию заявления о возбуждении уголовного дела, либо копию талона, содержащего порядковый номер из книги учета сообщений о преступлениях (далее – КУСП) содержащую отметку правоохранительного органа о его приеме, а также документы подтверждающие неправомерность списания денежных средств с расчетного счета. Обращаем внимание на то, что ходатайство необходимо направлять в суд по почте либо нарочно (отправка ходатайства через сервис «Мой арбитр» не допустима)
- Предпринять все меры для обеспечения сохранности и неизменности записей с внутренних и внешних камер систем видеонаблюдения, журналов систем контроля доступа, средств обеспечения и разграничения доступа в сеть Интернет за максимальный период времени, как до, так и после даты совершения хищения денежных средств.
- После окончания процедуры смены ключей не возобновлять деятельность на данной рабочей станции без проведения соответствующих технических мер, которые гарантируют полное уничтожение вирусных объектов. Если средствами антивирусных программ они не обнаружены, рекомендуется провести переустановку операционной системы с полным форматированием жесткого диска, но только в том случае, когда уже не требуется сохранение доказательной базы в целях проведения расследования инцидента правоохранительными органами и рассмотрения судебного иска. В случае необходимости сохранения персонального компьютера в текущем состоянии, использовать в работе другой компьютер с установленным лицензионным программным обеспечением (операционные системы, офисные пакеты и т.п.) и его автоматическим обновлением.

**За безопасное сотрудничество!**

**С уважением, Эс-Би-Ай Банк ООО.**