Ак Барс
Банк

АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «АК БАРС»
(публичное акционерное общество)

420066, Республика Татарстан,
г. Казань, ул. Декабристов, 1

+7 843 2-303-303
телекс: 224604ABBRU
akbars.ru

УТВЕРЖДАЮ
Управляющий директор Аппарата Правления
ПАО «АК БАРС» БАНК
_____Яшкин В.В.
«___» _____ 202__ г.
(с изменениями № 5853 от «25» июля 2022г.)

ИНСТРУКЦИЯ КЛИЕНТА ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПАО АК БАРС БАНК

П-5563 от 29.12.2021г.

Казань, 2022 г.

Оглавление

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В рамках настоящей Инструкции клиента по обеспечению информационной безопасности ПАО «АК БАРС» БАНК используются следующие термины и определения:

1.1. **Антивирусная проверка** – проверка файлов, системных областей компьютера, компьютерных сетей на наличие вредоносного программного обеспечения с использованием средств антивирусной защиты.

1.2. **Вредоносное программное обеспечение** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

1.3. **Клиент** – юридическое лицо, пользующееся услугами ПАО «АК БАРС» БАНК. Клиентом является лицо, обратившееся в банк для совершения кредитных, депозитных, расчетных, валютных и других банковских операций.

1.4. **Логин** – уникальная последовательность цифр, символов или латинских букв (строчных), определяемая Уполномоченным лицом Клиента самостоятельно, которая необходимая для его аутентификации в системе дистанционного банковского обслуживания.

1.5. **Мобильное устройство** – переносные малогабаритные электронные средства или системы, имеющие возможность размещения и обработки на них с помощью программного обеспечения информации, а также обмена этой информацией с другими электронными средствами или системами (смартфоны, планшеты).

1.6. **Переносное устройство** – персональный компьютер, имеющий небольшие габаритные размеры и вес, совмещающий в себе как внутренние элементы системного блока, так и устройства ввода-вывода (ноутбуки, нетбуки, ультрабуки).

1.7. **Пользователь** – это Клиент (Уполномоченное лицо Клиента), осуществляющий использование системы дистанционного банковского обслуживания.

1.8. **Программный комплекс PayControl** – программный комплекс, предназначенный для подтверждения Клиентом операций в системе дистанционного банковского обслуживания, а также для аутентификации Клиента при входе в систему, требующий установки специализированного программного обеспечения на мобильное устройство клиента. Средство подписи PayControl является простой электронной подписью.

1.9. **Система дистанционного банковского обслуживания (система ДБО)** – система электронного документооборота между Банком и Клиентом, представляющая собой совокупность каналов дистанционного банковского обслуживания «АК БАРС БИЗНЕС ОНЛАЙН» либо «АК БАРС БИЗНЕС ДРАЙВ». Вход в Систему возможен в сети Интернет по ссылке https://corp.akbars.ru либо через официальный сайт Банка www.akbars.ru Онлайн-банк.

1.10. **Система «АК БАРС МОБИЛЬНЫЙ» (Система МБК)** – канал информационного и платежного сервиса для работы с ЭД по счетам Клиента, требующий установки специализированного программного обеспечения на мобильное устройство Клиента. Является неотделимой частью канала «АК БАРС БИЗНЕС ОНЛАЙН» и «АК БАРС БИЗНЕС ДРАЙВ».

1.11. **Средство антивирусной защиты** – программное средство, определяющее наличие и предотвращающее действие вредоносного программного обеспечения.

1.12. **Стационарное устройство** – персональный компьютер, состоящий из отдельных конструктивно завершенных частей (системный блок, монитор, клавиатура и т.д.), соединенных интерфейсными кабелями. К стационарным компьютерам также относятся моноблоки – устройства, в которых все компоненты стационарного устройства конструктивно объединены в единое устройство, непредназначенное для переноски.

1.13. **Съемный носитель информации** – носитель, предназначенный для автономного хранения информации.

1.14. **Тарифы/Тарифный сборник** – совокупность банковских расходов, комиссий и вознаграждений, взимаемых Банком с Клиента за расчетно-кассовое обслуживание и предоставление услуг Клиенту в связи с обслуживанием счета Клиента, в том числе, но не ограничиваясь, за проведение операций по счету, ведение счета и его обслуживание по системе, тарифные планы, тарифные пакеты, а также за предоставление иных банковских продуктов и услуг, предоставляемых в рамках заключенных соглашений.

1.15. **Уполномоченное лицо Клиента** – представитель Клиента, уполномоченный работать в Системе с соблюдением требований действующего законодательства Российской Федерации, наделенный правом распоряжаться денежными средствами на счете, а также полномочиями по подписанию документов, совершению иных действий в рамках реализованных услуг в Системе ДБО.

1.16. **Электронный документ** – электронный образ документа (платежного или иного), представленный в согласованном сторонами формате, определяемом программными средствами создания документа. Электронный документ передается между сторонами в составе файла, подписанного электронной подписью. В состав файла может входить несколько электронных документов. Если файл имеет корректную электронную подпись, то каждый электронный документ, входящий в файл, считается подписанным электронной подписью.

1.17. **Электронная подпись** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1.18. **SMS-код** – буквенно-цифровой код, направляемый в виде SMS-сообщения на номер мобильного телефона Клиента или Уполномоченного лица Клиента. Действителен для применения в течение определенного периода времени, по истечении которого, если им не воспользоваться, становится недействителен. Буквенно-цифровой SMS-код используется для входа в Систему ДБО.

1.19. **Рутокен** – персональное устройство хранения электронной подписи с усиленной безопасностью.

1.20. **eTokenPass** – автономный генератор одноразовых паролей, не требующий подключения к компьютеру и установки дополнительного программного обеспечения.

1.21. **RDP (Remote Desktop Protocol)** – протокол подключения пользователя к удаленному рабочему столу.

1.22. **SafeTouch Pro** – устройство визуализации и контроля подписываемых документов.

Используемые сокращения

БАНК – ПАО «АК БАРС» БАНК.
ДБО – Дистанционное банковское обслуживание.
ДПИБ – Департамент по информационной безопасности.
ИБ – Информационная безопасность.
Инструкция – Инструкция клиента по обеспечению информационной безопасности ПАО «АК БАРС» БАНК.
ПО – Программное обеспечение.
СНИ – Съемный носитель информации.
RDP – Remote Desktop Protocol.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Целью настоящей Инструкции является определение требований по обеспечению ИБ при работе Клиентов в Системе ДБО.

2.2. Настоящая Инструкция разработана в соответствии с требованиями и рекомендациями национальных и международных нормативно правовых актов, а также требованиями внутренних нормативных документов Банка и соглашений на подключение и обслуживание Системы ДБО.

2.3. Владельцем настоящей Инструкции является ДПИБ.

2.4. Настоящая Инструкция является обязательной для исполнения Клиентами Банка и подлежит публикации на официальном сайте Банка https://www.akbars.ru**.**

2.5. Клиент несет персональную ответственность за соблюдение настоящей Инструкции.

3. ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К УСТРОЙСТВАМ, С КОТОРЫХ ОСУЩЕСТВЛЯЕТСЯ ДОСТУП К СИСТЕМЕ ДБО

3.1. Стационарное устройство/переносное устройство должно быть защищено специализированными средствами защиты информации, а именно средствами антивирусной и сетевой защиты (персональный фаервол), разрешающие доступ в сеть Интернет только тем программам, которые необходимы для работы с Системой ДБО, и запрещающие любые иные обращения к стационарному устройству/переносному устройству из сети Интернет, в том числе и его подключение к сетям общего доступа в местах свободного доступа в Интернет (офисные центры, кафе и пр.).

3.2. На стационарном устройстве/переносном устройстве, с которого осуществляется доступ к Системе ДБО:

–должна быть установлена только одна операционная система, а также рекомендуется устанавливать только те программы, которые необходимы для работы в Системе ДБО;

–запрещается устанавливать иное ПО, содержащее средства разработки и отладки приложений, а также средства, позволяющие осуществлять несанкционированный доступ к системным ресурсам;

–запрещается устанавливать ПО, полученное из непроверенных источников;

–должны быть отключены все неиспользуемые для связи с Банком службы и процессы операционной системы Windows, в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, а именно:

- отключить возможность терминального соединения с компьютерами, используемыми для работы по Системе ДБО – заблокировать порт, используемый для подключений по RDP-протоколу (по умолчанию 3389);
- отключить "Гостевой доступ" – заблокировать локальную учетную запись «Гость» (Guest);

–должно устанавливаться только лицензионное ПО;

–версия операционной системы должна быть актуальной;

–должны своевременно устанавливаться обновления операционной системы, а также обновления по безопасности прикладного ПО;

–должно быть установлено лицензионное средство антивирусной защиты (предпочтительно российского производителя) со своевременно обновляемыми антивирусными базами данных и проверкой по расписанию всех объектов системы;

–должна быть активирована подсистема регистрации событий ИБ;

–пользователи не должны обладать правами локального администратора;

–на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям раздела 4 настоящей Инструкции;

–должно быть исключено подключение СНИ, не участвующих в работе Системы ДБО.

3.3. На мобильном устройстве, с которого осуществляется доступ к Системе ДБО:

–версия операционной системы должна быть актуальной (соответствовать требованиям для установки и использования Системы ДБО и иного ПО Банка, необходимого для полноценного функционирования Системы ДБО);

–запрещается получать неограниченный доступ (права суперпользователя) к системным файлам и другим ресурсам мобильного устройства;

–рекомендуется устанавливать только необходимое ПО;

–запрещается устанавливать ПО из недостоверных источников;

–запрещается устанавливать сертификаты безопасности из ненадежных источников;

–должно быть установлено лицензионное средство антивирусной защиты (предпочтительно российского производителя) со своевременно обновляемыми антивирусными базами данных и проверкой по расписанию всех объектов системы.

3.4. При разблокировки мобильного устройства должен быть включен один из способов защиты от несанкционированного доступа к функциям мобильного устройства и хранящихся на нём данным:

–биометрические средства защиты (средства распознавания отпечатка пальца или лица);

–пароль;

–графический ключ;

–пин-код.

3.5. Рекомендуется комбинировать способы защиты от несанкционированного доступа, указанные в пункте 3.4 настоящей Инструкции.

3.6. Настройку стационарного устройства/переносного устройства (управление привилегиями, квотами, установка прав доступа пользователей и т.п.) должен выполнять специалист, обладающий необходимыми навыками по администрированию компьютерной техники и сети.

3.7. Устройства, с которых осуществляется доступ к Системе ДБО, рекомендуется располагать в помещении, в котором исключен несанкционированный доступ.

4. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИБ, ПРЕДЪЯВЛЯЕМЫЕ К ПАРОЛЯМ

4.1. При выборе пароля необходимо соблюдать следующие требования:

– пароль должен содержать не менее 8 символов;

– пароль должен содержать как минимум по одному символу из букв нижнего и верхнего регистра, цифры и знаки препинания;

– не использовать в качестве пароля один и тот же повторяющийся символ, либо комбинацию из нескольких рядом стоящих символов;

– не использовать в качестве пароля имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, девичью фамилию матери и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о клиенте.

4.2. Пароль от операционной системы и пароль для входа в систему ДБО необходимо менять один раз в 90 календарных дней. Запрещено ставить один и тот же пароль на операционную систему и систему ДБО.

4.3. Строго запрещается записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в легкодоступных местах, передавать неуполномоченным лицам.

4.4. Пароль должен быть немедленно изменен в случае компрометации или подозрения на компрометацию.

5. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИБ, ПРЕДЪЯВЛЯЕМЫЕ К КЛЮЧЕВОЙ ИНФОРМАЦИИ КЛИЕНТА

5.1. Ключевая информация для работы в системе ДБО на стационарном устройстве/переносном устройстве (ключ электронной подписи для работы в Системе ДБО) должна размещаться на СНИ (eToken Pass, Рутокен и Safe Touch Pro). Размещение ключевой информации на жестком диске, на котором установлена Система ДБО, запрещено.

5.2. СНИ с ключевой информацией должен быть установлен в считывающее устройство только во время работы в Системе ДБО. Размещение СНИ в считывающем устройстве вне сеансов работы в Системе ДБО должно быть исключено.

5.3. СНИ с ключевой информацией должен использоваться только владельцем сертификата ключа проверки электронной подписи либо лицом, уполномоченным на использование такого сменного носителя.

5.4. Хранить СНИ с ключевой информацией необходимо в защищаемой комнате, в сейфе (металлическом ящике), исключающей доступ неуполномоченных лиц и повреждение материального носителя. Вся ответственность за конфиденциальность секретных ключей электронной подписи лежит на Клиенте, как на единственном владельце секретных ключей электронной подписи.

5.5. Не допускается:

– снимать несанкционированные копии с СНИ с ключевой информации;

– передавать носители ключевой информации лицам, которые к ним не допущены;

– записывать на носители ключевой информации постороннюю информацию.

5.6. Для подтверждения операций в Системе ДБО с помощью мобильного устройства используется приложение PayControl.

5.7. При добавлении ключа в мобильное приложение PayControl необходимо установить способ защиты ключа с использованием пароля, отвечающего требования по безопасности, указанные в разделе 4 настоящей Инструкции или систем распознавания отпечатка пальца или лица (при наличии такой функциональной возможности на мобильном устройстве).

5.8. В случае, если при запуске мобильного приложения PayControl будет выведено уведомление, о том, что на мобильном устройстве обнаружено подозрительное ПО, необходимо убедится в надёжности этого ПО и при необходимости удалить перечисленное в этом уведомлении ПО, и лишь после этого продолжать работу с мобильным приложением PayControl.

6. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

6.1. Пользователю не рекомендуется оставлять включенные устройства, с которых осуществляется доступ к Системе ДБО, без контроля. Недопустимо отлучаться от устройств, с которых осуществляется доступ к Системе ДБО, во время сеанса связи с Банком. Время до автоматической блокировки экрана во время бездействия Пользователя должно составлять не более 3 минут. Разблокировка экрана должна происходить по паролю.

6.2. Пользователю не рекомендуется работать в Системе ДБО в Интернет-кафе, библиотеках и других местах с публичным доступом в сеть Интернет из-за невозможности обеспечить требования по ИБ в вышеперечисленных заведениях.

6.3. Пользователь должен исключить попадание вредоносных программ и неправомерный доступ неуполномоченных лиц на устройства, с которых осуществляется доступ к Системе ДБО.

6.4. Клиент обязан соблюдать требования настоящей Инструкции, а также изучать рассылки от Банка по вопросам защиты информации от воздействия вредоносного кода, о возможных рисках и мерах по их снижению, в том числе информации о:

– рекомендуемых мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого Клиентом осуществлялся перевод денежных средств;

– рекомендуемых мерах по контролю конфигурации устройства, с использованием которого Клиентом осуществляется перевод денежных средств, и своевременному обнаружению воздействия вредоносного кода;

– появлении в сети Интернет ложных (фальсифицированных) ресурсов и ПО, имитирующих программный интерфейс Банка по переводу денежных средств, и рекомендуемых мерах по обнаружению указанных ресурсов и программного обеспечения.

6.5. Пользователю при осуществлении доступа к Системе ДБО необходимо удостовериться в правильности указанного адреса в адресной строке браузера (должно быть https://corp.akbars.ru) и значок защищенного соединения (замок), исключая выход на сайты, внешне маскирующиеся под Интернет-Банк.

6.6. Отправление электронных платежных документов необходимо производить только с использованием идентификационной информации, используемой для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, ПО с целью осуществления переводов денежных средств, которой в зависимости от технической возможности является IP-адрес, MAC-адрес и (или) иной идентификатор устройства.

6.7. Клиент обязан соблюдать требования настоящей Инструкции, рекомендации Банка, а также требования иных документов, размещенных на официальном сайте Банка по адресу https://www.akbars.ru.

7. ДЕЙСТВИЯ КЛИЕНТА ПРИ ПОЛУЧЕНИИ СООБЩЕНИЙ ИЗ БАНКА И КОМПРОМЕТАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ

7.1. Клиент ни при каких случаях не должен отвечать на письма, направленные якобы от имени Системы ДБО, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену https://www.akbars.ru, переслать секретный ключ, пароль доступа к системе или сеансовый ключ, и обязан немедленно сообщить о подобном факте администратору Системы ДБО Банка по телефонам технической поддержки: (843) 239-73-38 или 8-800-2005-304.

7.2. Банк информирует клиента, что не осуществляет рассылку электронных писем с просьбой прислать ключи электронной подписи или пароль. Банк не рассылает по электронной почте программы для установки на компьютеры клиента.

7.3. В случае поступления на мобильный номер телефона клиента SMS-оповещения или электронного сообщения о совершенной операции, которая не была совершена Клиентом, необходимо немедленно связаться с Банком по соответствующим каналам и телефонам, указанным п.7.1. настоящей Инструкции, или лично.

7.4. При подозрении на компрометацию ключевой информации, в случаях кадровых перестановок лиц, имевших доступ к Системе ДБО, компьютеру и ключам, при опасениях в несанкционированном доступе, при случаях обнаружения вируса Клиенту необходимо немедленно обратиться в Банк по телефонам: (843) 239-73-38, 8-800-2005-304, либо лично явиться в Банк, с целью блокирования скомпрометированных секретных ключей электронной подписи с последующей их заменой.

8. МЕРЫ ЗАЩИТЫ

8.1. Клиент должен защищать электронные документы, поставляемые в Банк по Системе ДБО средствами защиты информации на выбор с помощью Рутокен и/или Программного комплекса PayControl.

8.2. Клиент вправе ограничить работу Системы ДБО с одного или нескольких устройств, с использованием которых может осуществляться доступ к Системе ДБО с целью осуществления переводов электронно-платежных/электронных документов, на основе идентификаторов MAC-адресов. При осуществлении режима работы с любых MAC-адресов Клиент понимает и принимает на себя все риски, связанные с возможностью доступа к серверу Системы ДБО с любого компьютера при наличии доступа к ключам электронной подписи и паролям.

8.3. Клиент вправе дополнительно выбрать предоставляемую Банком возможность, услугу по дополнительному информированию по альтернативному каналу связи (мобильный телефон, электронная почта) о каждой отправке электронно-платежных документов в Банк.

8.4. Заявление намерения клиента использовать дополнительную услугу по альтернативным каналам связи и номера мобильных телефонов для приема SMS-сообщений оформляются в соответствующем соглашении по форме Банка и подлежит оплате в соответствии с Тарифами Банка.

8.5. Клиент вправе на основании заявления выбрать предоставляемую Банком возможность определять дополнительные ограничения (параметры) операций, которые могут осуществляться клиентом с использованием Системы ДБО, устанавливать ограничение:

– на максимальную сумму перевода денежных средств за одну операцию;

– на общую сумму переводов денежных средств за определенный период времени в днях.

8.6. Клиент (уполномоченное лицо Клиента) вправе, на основании заявления, выбрать предоставляемую Банком возможность использования одноразового кода подтверждения, в целях двухфакторной аутентификации пользователя Клиента, реализованного путем отправки SMS-сообщений на номер мобильного телефона или выработанного кода Программным комплексом PayControl, или в виде подключения специального технического устройства eTokenPass, с оплатой согласно Тарифам Банка.