

Рекомендации для клиентов юридических лиц и индивидуальных предпринимателей по мерам снижения риска получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, а также рекомендации по защите информации от воздействий вредоносного кода.

В целях выполнения требований Положения Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», рекомендаций, изложенных в письмах от 7 декабря 2007 г. № 197-Т «О рисках при дистанционном банковском обслуживании», от 30 января 2009 г. № 11-Т «О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга», от 25 июня 2009 г. № 76-Т «О рекомендациях по информированию клиентов о размещении на Web-сайте Банка России списка адресов Web-сайтов кредитных организаций», от 23 октября 2009 г. N 128- Т «О Рекомендациях по информационному содержанию и организации Web-сайтов кредитных организаций в сети Интернет», от 5 августа 2013 г. № 146-Т «Рекомендации по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети «Интернет» ООО банк «Элита» (далее - Банк) доводит до своих Клиентов информацию о существующих рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, а также приводит список рекомендаций по защите информации от воздействия вредоносного кода (компьютерные вирусы, «трояны», «руткиты» и т.п.), о мерах соблюдения информационной безопасности и способах пресечения хищения.

Технологии защиты операций в Системе дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей (далее – СДБО) используют современные механизмы обеспечения безопасности и предоставляют удобство пользования услугой, обеспечивая при этом высокий уровень её надёжности и безопасности.

Безопасность и защита от несанкционированного доступа в СДБО обеспечивается применением:

- средств электронной подписи (СКЗИ). Поддерживается СКЗИ производства ведущего отечественного разработчика «Сигнал-Ком» – сертифицированная криптобиблиотека «Message-PRO v.4.0.x» на базе СКЗИ «Крипто-КОМ 3.3» для обеспечения криптографической защиты информации при использовании ключей электронной подписи;
- протоколов безопасности SSL и TLS, позволяющих повысить надёжность связи и защитить передаваемую информацию от несанкционированного доступа с помощью сертификатов Geotrust True BusinessID EV с расширенной проверкой (сертификаты EV имеют максимальный уровень доверия и визуально подтверждают высокую надёжность сайта, выделяя его зеленым цветом в адресной строке);
- многофакторной аутентификации, авторизации, протоколирования;

- межсетевое экранирование, сертифицированного ФСТЭК России;
- штатных средств защиты операционной системы и баз данных;
- дополнительных средств эшелонированной защиты от воздействия вредоносного кода сертифицированных ФСТЭК России;
- организационно-административных мероприятий;
- систем контроля доступа.

Хищение денежных средств с расчётных счетов Клиента возможно при получении злоумышленниками тем или иным образом доступа к Ключевому носителю Клиента, логину и паролю, с целью направления в Банк платёжных поручений, заверенных от лица Клиента, что предположительно могут осуществить:

- ответственные сотрудники организации Клиента, ранее имевшие доступ к Ключевому носителю для работы с СДБО, например, уволенные директора, бухгалтеры и их заместители, а также совладельцы организации;
- штатные сотрудники технической поддержки организации Клиента, имеющие или имевшие ранее технический доступ к Ключевому носителю, а также доступ к компьютерам организации, с которых осуществлялась работа в СДБО;
- нештатные, приходящие по вызову, сотрудники технической поддержки, обслуживающие компьютеры организации Клиента, осуществляющие профилактику и подключение к сети Интернет, установку и обновление бухгалтерских и информационно-правовых программ, установку, обновление и настройку другого программного обеспечения на компьютерах, с которых осуществлялась или осуществляется работа в СДБО;
- злоумышленники (неустановленные лица), получившие несанкционированный доступ к компьютерам организации Клиента, с которых осуществляется доступ в СДБО, из внешней сети (например, из сети интернет);
- сотрудник организации Клиента, не уделивший должного внимания при проверке реквизитов подписываемых документов, может поставить электронную подпись под документом, сформированным злоумышленником и непреднамеренно отправить его в Банк.

Таким образом, в Банк могут поступать не вызывающие подозрений платежи, направленные злоумышленниками с использованием корректной и действующей электронной подписью Клиента, имеющие обычные реквизиты получателей и типовые назначения платежа. Правомерное, в данном случае, исполнение таких платежей Банком приведёт к хищению денежных средств со счета Клиента.

Банк не имеет доступа к Ключевому носителю Клиента с рабочими ключами электронной подписи (далее – ЭП) и не может от его имени сформировать корректную электронную подпись под Электронным документом. Банк не осуществляет рассылку электронных писем посредством электронной почты с просьбой к Клиенту предоставить какую-либо информацию Клиента по его работе в СДБО, в том числе парольную информацию. Банк не рассылает по электронной почте программы для установки на компьютеры Клиентов.

В целях обеспечения безопасности при работе в СДБО, необходимо строго соблюдать рекомендации по информационной безопасности, ограничить доступ к компьютерам Клиента, с которых осуществляется работа в СДБО.

Клиентам необходимо учитывать, подготовленные Банком, следующие **рекомендации для снижения рисков получения несанкционированного доступа:**

- Рекомендуется выделить отдельный компьютер, который использовать только для работы с СДБО;
- Исключить доступ к компьютерам для работы с СДБО персонала, не имеющего отношения к работе с СДБО;
- Размещение, охрана и специальное оборудование помещения, в котором установлены компьютеры, используемые для доступа в СДБО, должны обеспечивать сохранность информации, исключать возможность неконтролируемого проникновения в это помещение;
- Принять меры по контролю конфигурации компьютера, с использованием которого осуществляется перевод денежных средств через СДБО, и её изменения. Не допускать несанкционированных программно-аппаратных изменений конфигурации;
- На компьютере для работы с СДБО необходимо использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечить регулярную своевременную установку обновлений, выпускаемых разработчиками СДБО, операционной системы, web-браузеров (Microsoft Internet Explorer, Mozilla FireFox, Opera и т.д.) и иного прикладного программного обеспечения;
- Применять на компьютере для работы с СДБО лицензионные средства антивирусной защиты, обеспечить регулярное автоматическое обновление компонентов антивирусной защиты;
- Рекомендуется применять на компьютере для работы с СДБО 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;
- На компьютере для работы с СДБО необходимо исключить посещение WEB- сайтов сомнительного содержания, загрузку и установку нелегального программного обеспечения и т.п. Использование нелегального программного обеспечения повышает риск получения несанкционированного доступа злоумышленников с целью хищения денежных средств;
- Не допускается работать с СДБО 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;
- Установить пароли на учётные записи пользователей операционной системы на компьютере для работы с СДБО. Работу с СДБО на компьютере осуществлять только под учетной записью с ограниченными правами в операционной системе. Не допускать штатную работу в СДБО под учетной записью с правами администратора в операционной системе компьютера;
- Не разглашать логин и пароль от СДБО никому, в том числе лицам, представившемся сотрудниками Банка. Банк не рассылает по открытым каналам связи электронных писем, SMS или других сообщений с просьбой уточнить данные Клиента. Используемые в СДБО логин и пароль, запрещается записывать и хранить в местах, доступных посторонним лицам. Не пересылайте логин и пароль от СДБО по электронной почте или SMS сообщениями;

- 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 ООО банк «Элита» или СДБО, пожалуйста, незамедлительно сообщите об этом по контактными телефонам Банка. Список адресов (доменных имен) официальных WEB-сайтов Банка размещен на сайте Банка России по адресу http://www.cbr.ru/credit/CO_SitesFull.asp;

- Во избежание использования ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемой Банком СДБО, 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 СДБО. Для этого необходимо переходить на страницу СДБО по ссылке «ЮРИДИЧЕСКИМ ЛИЦАМ» с официального Интернет- ресурса Банка – <https://www.bankelita.ru>. Прежде чем ввести логин и пароль, Клиентам Головного офиса необходимо проверить по информации из SSL-сертификата подлинность сайта [dbo.bankelita.ru](https://www.bankelita.ru). Для этого в адресной строке браузера, например, Internet Explorer, щёлкните мышкой на символ замка, далее «Просмотр сертификатов», перейти на закладку «Состав», встать на строку «Субъект», в окне просмотра убедитесь в наличии следующей информации: CN = [dbo.bankelita.ru](https://www.bankelita.ru)
OU = The information security office O = LLC bank "ELITA" L = Kaluga S = Kaluzhskaya obl.
C = RU

. Аналогичным образом можно посмотреть эту информацию и в других браузерах. Центром сертификации, подтверждающим подлинность сайтов [dbo.bankelita.ru](https://www.bankelita.ru), является GeoTrust EV SSL CA - G4;

- Работу с СДБО рекомендуется осуществлять с использованием технических средств с индивидуальными дистанционно распознаваемыми идентификационными признаками (IP- и MAC-адреса), предоставленными в Банк;

- При создании паролей придерживайтесь следующих правил. Не допускается использовать в качестве пароля простые, легко угадываемые комбинации букв и цифр, а также пароли, используемые для доступа в другие СДБО. Пароль должен соответствовать следующим требованиям – длина пароля должна быть не менее 8 символов, в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, %, и т.п.), пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, год рождения, номер телефона и т.п.);

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

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

- Использование Ключевого носителя должно осуществляться исключительно владельцем ключа ЭП и храниться в месте, защищённом от доступа третьих лиц (например: сейф, запирающийся на ключ металлический ящик);

- Необходимо отключать, извлекать Ключевой носитель, если он не используется для работы в СДБО. Размещение Ключевого носителя в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключам ЭП третьими лицами;
- 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;
- Регулярно проводить контроль сумм и получателей электронных документов в информационном окне СДБО, а также контролировать количество и сумму отправленных электронных документов;
- Регулярно контролировать состояние своих счетов и незамедлительно сообщать в Банк обо всех подозрительных или несанкционированных изменениях;
- При обслуживании компьютера сотрудниками технической поддержки организации Клиента или сторонних организаций – обеспечивать контроль выполняемых ими действий;
- Не передавать Ключевой носитель сотрудникам технической поддержки для проверки работы СДБО, 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 СДБО, и лично ввести пароль, не допуская ознакомления с ним посторонних лиц;
- В случае передачи (списания) компьютера, на котором ранее была установлена СДБО, 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 СДБО;
- 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.
- Необходимо корректно завершать работу в СДБО, используя для этого пункт меню «Выйти из системы».

Рекомендации по защите информации от воздействий вредоносного кода:

- Необходимо применять на компьютере, с которого ведётся работа с СДБО, лицензионные средства антивирусной защиты, работающие в автоматическом режиме;
- В обязательном порядке обеспечить на постоянной основе автоматическое обновление антивирусных баз;
- Осуществлять регулярный контроль функционирования системы антивирусной защиты;
- Отключение антивирусных средств или несвоевременное обновление, установленных на компьютерах с которых производятся работы в СДБО, категорически не допускается. В случае обнаружения на компьютере нештатного отключения антивирусных средств – не допускается работа с СДБО на этом компьютере до устранения причины нештатного отключения;
- Необходимо осуществлять проверку компьютера на наличие вредоносного кода перед началом работы с СДБО и установкой программного обеспечения СДБО, а также в следующих случаях: при увольнении штатного сотрудника технической поддержки

организации, осуществляющего обслуживание компьютера, с которого ведётся работа с СДБО; после доступа к компьютеру внештатных сотрудников технической поддержки организации или любых других работников, выполнивших работу по установке, обновлению и поддержке различных бухгалтерских, правовых, информационных и других программ.

- Необходимо на постоянной основе регулярно, например, ежемесячно, проводить полную проверку компьютера, на котором ведётся работа с СДБО, на наличие вредоносного кода.

- На компьютерах, используемых для работы с СДБО, исключить посещение Интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т. п.;

- Исключить использование любого программного обеспечения развлекательного и социального характера и др., за исключением необходимого для работы с СДБО;

- Перейти к использованию лицензионного программного обеспечения (операционные системы, офисные пакеты и пр.), обеспечить автоматическое обновление системного и прикладного программного обеспечения;

- Обеспечить применение и использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации путём использования уязвимостей программного обеспечения;

- Необходимо применять на рабочем месте специализированные программные средства безопасности: персональные фаерволы, антишпионское программное обеспечение и т.п.;

- На компьютере, на котором установлена СДБО, запрещается открытие и исполнение файлов, не требующихся при работе с СДБО, в том числе полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них вредоносного кода.

- Необходимо обеспечить защиту компьютера от внешнего сетевого доступа программным или аппаратным средством межсетевого экранирования;

- В случае выхода из строя рабочего компьютера, либо некорректной работы СДБО, или признаков наличия вредоносного кода, а также нестандартного поведения компьютера, при работе с Ключевым носителем – необходимо незамедлительно прекратить работу на ПК, извлечь Ключевой носитель и обратиться в Банк.