

Правила безопасности при работе в системе дистанционного банковского обслуживания физических лиц в ООО банк «Элита»

В целях выполнения требований Положения Банка России от 17 августа 2023г. N 821-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 27 декабря 2021 г. № ИН-03-23/104 «О размещении на сайте Банка России в сети «Интернет» информационного ресурса, содержащего перечень требований и рекомендаций по раскрытию информации на сайтах финансовых организаций и об отмене письма Банка России от 23.10.2009 № 128-Т», от 5 августа 2013 г. № 146-Т «Рекомендации по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети «Интернет», от 28 февраля 2024 г. N 3-МР «Методические рекомендации по усилению кредитными организациями информационной работы с клиентами в целях противодействия осуществлению переводов денежных средств без добровольного согласия клиента» 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 (далее – СДБО Интернет-банк) 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 Интернет-банк обеспечивается применением:

- протоколов безопасности SSL и TLS, позволяющих повысить надёжность связи и защитить передаваемую информацию от несанкционированного доступа с помощью сертификатов GlobalSign OrganizationSSL Wildcard;
- 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.

Заходите в СДБО Интернет-банк только с официального сайта. Убедитесь, что Вы находитесь на подлинном сайте и адрес в поле «адрес» или «узел» Вашего браузера соответствует официальному адресу веб-сайта <https://online.bankelita.ru/>

Прежде чем пройти авторизацию в СДБО Интернет-банке, убедитесь, что соединение происходит в защищенном режиме с использованием протокола HTTPS (появляется буква S в адресной строке: <https://online.bankelita.ru/>), удостоверьтесь в правильности сертификата SSL-соединения, убедитесь в наличии пиктограммы закрытого замка на панели в левом верхнем углу веб-страницы (в адресной строке) перед осуществлением передачи конфиденциальной информации через вебсайт. Данный символ указывает на то, что сайт работает в защищенном режиме, и все передаваемые данные будут защищены. Ссылка для входа в Интернет-банк указана на сайте Банка <http://bankelita.ru/> .

Не пользуйтесь СДБО Интернет-банк в общедоступных местах, на компьютерах, безопасность которых вызывает сомнения (например, в Интернет-кафе, чужой компьютер). Если Вы все же заходили с чужого компьютера, смените пароль для входа в СДБО Интернет-банк с Вашего персонального компьютера, как только будет такая возможность.

Не отвечайте на телефонные звонки (особенно поступившие с использованием мессенджеров), сообщения в мессенджерах, СМС-сообщения, содержащие запрос о вашей конфиденциальной информации (пароль, одноразовые пароли (Push/СМС-пароли), данные о банках, услугами которых вы пользуетесь, и так далее).

Никому не говорите Ваш пароль и одноразовый пароль. Помните, что сотрудники Банка никогда не просят сообщить или ввести куда-либо конфиденциальную информацию (Pin-код, пароль или одноразовый пароль, полученный по SMS).

Внимательно просматривайте текст приходящих на ваше мобильное устройство одноразовых паролей, чтобы убедиться, что вы подтверждаете выполнение именно той операции, которую собирались совершить.

Не вводите свой номер паспорта и другие данные при входе в СДБО Интернет-банк или подтверждении операций. Если от Вас требуется ввод любой другой персональной информации (номер банковской карты, СVC-код или других личных данных), следует прекратить пользование услугой и связаться с Банком для блокировки учетной записи.

Вирусные программы могут запоминать и отсылать всю информацию злоумышленникам. Установите современное антивирусное программное обеспечение предпочтительно российского производства и следите за его регулярным обновлением для своевременного обнаружения вредоносных программ.

Установите или используйте встроенный брандмауэр (firewall) для входа в Интернет, это позволит предотвратить несанкционированный доступ к информации на Вашем компьютере.

Не пользуйтесь СДБО Интернет-банк на компьютере, который используется под учетной записью, имеющей права администратора системы, а также если имеется подозрение, что компьютер заражен вирусной программой. Симптомы заражения:

- на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы;
- произвольно, без участия пользователя, на компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ выйти в Интернет, хотя пользователь этого не инициировал;
- частые зависания и сбои в работе компьютера, медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы, исчезновение файлов и каталогов или искажение их содержимого.

Для завершения работы с СДБО Интернет-банк не выходите из СДБО Интернет-банк закрытием браузера. В целях обеспечения сохранности Ваших данных необходимо осуществлять выход из СДБО Интернет-банк нажатием ссылки «Выход» в верхней части рабочей области экрана.

При работе с СДБО через мобильное приложение следует выполнять следующие рекомендации для владельцев смартфонов:

- установите пароль на доступ к Вашему мобильному устройству. Используйте сложный пароль или пин-код. Средства блокировки по простому графическому ключу или фотографии не обеспечивают должного уровня защиты.

- не используйте мобильные устройства с расширенными правами (Jailbreak, Root или иные операции, не поддерживаемые официально производителями).

- установите на Вашем мобильном устройстве и регулярно обновляйте мобильный антивирус (рекомендуется использовать антивирус российского производителя, так как он учитывает региональную специфику вредоносного ПО).

- своевременно устанавливайте обновления для Вашего мобильного устройства и установленных на нем приложений. Установку производите только из доверенных источников (Google Play Market и Apple AppStore, Huawei AppGallery, маркеты производителей устройств и т.п.). Иные способы установки приложений и обновлений небезопасны. Недопустима установка или обновление приложений по ссылке в e-mail / SMS-сообщении от имени Банка. Обратите внимание: Банк никогда не высылает писем и SMS-сообщений с прямыми ссылками на установку или обновление приложений.

- при установке на Ваше мобильное устройство дополнительного программного обеспечения обращайте внимание на полномочия, которые необходимы программе. Не допускайте установки программ, которым требуются излишние полномочия, особенно в части чтения и отправки SMS-сообщений, доступа к сети Интернет, клавиатуре и т.п.

- если Вы заметили, что на Ваше мобильное устройство перестали приходить SMS, в том числе перестали приходить SMS-пароли от Банка, необходимо прекратить использование мобильного устройства. В данном случае возможно мошенничество с заражением Вашего мобильного устройства вирусом, перехватывающим SMS-сообщения. Для проверки рекомендуем установить SIM-карту в другое мобильное устройство, провести операцию в Системе и дождаться прихода SMS-пароля. Так же о заражении вирусом может свидетельствовать подозрительная работа устройства (самопроизвольные звонки и рассылки SMS, несанкционированная загрузка и установка программного обеспечения). В случае выявления данных фактов рекомендуем обратиться за помощью в службу технической поддержки производителя Вашего мобильного устройства.

Одним из способов мошеннических действий является рассылка писем с указанием ссылок на поддельные web- сайты, имеющие похожие адреса, или перенаправление на них с других ресурсов. Внимательно проверяйте адрес сайта перед авторизацией или совершением операций. Если он отличается от <https://online.bankelita.ru> – не используйте данный сайт. Для входа в Интернет-банк перейдите по ссылке с сайта Банка <http://bankelita.ru/> или наберите адрес в браузере вручную.

Если у вас есть подозрение, что Ваши учетная запись и пароль украдены, как можно быстрее смените пароль в СДБО Интернет-банк или заблокируйте доступ в систему через службу поддержки +7 (4842) 27-74-20, доб. 122, 124, электронная почта: support@bankelita.ru