

Рекомендации для клиентов, частных лиц 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 (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 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;
- межсетевого экранирования, 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/v1/cgi/bsi.dll?T=RT_2Auth.BF

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. 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.

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).

Для входа в СДБО Интернет-банк необходимо указывать только логин (учетная запись) и пароль. Не вводите свой номер телефона, 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, мобильного телефона 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 антивирус (средство защиты от воздействия вредоносного кода) на Вашем компьютере и своевременно обновляйте антивирусные базы данных.

Установите и используйте персональный 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.

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) 57-10-56 или +7 (4842) 53-19-51