Требования

по обеспечению информационной безопасности при работе в системе «ВТБ Бизнес Онлайн»

Приложение № 2
к Условиям комплексного обслуживания Клиентов
с использованием системы «ВТБ Бизнес Онлайн»

1. Требования по обеспечению информационной безопасности компьютера, с которого осуществляется работа в системе «ВТБ Бизнес Онлайн».

1.1. Компьютеры должны располагаться в помещениях, обеспечивающих невозможность несанкционированного доступа к ним или должен быть обеспечен режим эксплуатации компьютера, исключающего доступ к нему неуполномоченных лиц.

1.2. Правом доступа к компьютерам должны обладать только лица, ознакомленные с настоящими требованиями и с другими нормативными документами, регламентирующими работу в системе «ВТБ Бизнес Онлайн».

1.3. Запрещается оставлять без контроля компьютер при включенном питании и загруженном программном обеспечении. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана должно производиться с использованием пароля доступа.

1.4. Рекомендуется подключать компьютер к сети электропитания через устройства бесперебойного питания.

1.5. На компьютере должна быть установлена только одна операционная система и только те программы, которые необходимы в работе с системой «ВТБ Бизнес Онлайн». Рекомендуется настроить такой режим работы, чтобы исключить запуск любых иных программ, кроме тех которые необходимы в работе с системой «ВТБ Бизнес Онлайн».

1.6. Программное обеспечение, установленное на компьютере, не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

1.7. Компьютеры должны быть защищены с помощью специальных программных или аппаратных средств антивирусной защиты (сетевых или персональных) и сетевой защиты (персональные фаерволы), разрешающие доступ к Интернет только тем программам, которые необходимы для работы с системой «ВТБ Бизнес Онлайн» и запрещающие любое несанкционированное обращение к компьютеру из сети Интернет.

1.8. Не рекомендуется использовать компьютер, с которого ведется работа в системе «ВТБ Бизнес Онлайн», для иных целей.

1.9. Необходимо регулярно производить обновления антивирусных баз, а также обновления по безопасности прикладного программного обеспечения, установленного на компьютере (включая обновление антивирусных систем, фаервола, офисных программных приложений и т.п.), а также обновления операционной системы.

1.10. Не следует исполнять и открывать файлы, полученные из сети Интернет или через съемные носители, без проведения предварительной их проверки на предмет содержания в них программных закладок и вирусов.

1.11. На компьютере должна быть установлена парольная защита на вход в BIOS и в операционную систему. При выборе пароля необходимо следовать следующим рекомендациям:

- пароль должен содержать не менее 6 символов;
- не использовать в качестве пароля имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об администраторе или пользователе;
- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567» или «1йфячыц2» и т. п.);

- использовать в качестве пароля комбинацию знаков, смысл последовательности которых трудно определить.

1.12. Настройку компьютера (управлению привилегиями, квотами, установке прав доступа пользователей и т.п.) должен выполнять специалист, обладающий необходимыми навыками по администрированию компьютерной техники и сети. Пользователи при работе с системой «ВТБ Бизнес Онлайн» не должны обладать правами локального администратора на компьютере.

2. Требования по обеспечению информационной безопасности при хранении и использовании Ключевой информации.

2.1. Использование средств электронной подписи и Ключевой информации допускается в целях, определенных в Договоре и настоящем Соглашении.

2.2. Если Ключевая информация хранится на отдельных носителях (дискеты, флешки, USB-токены и тп.), то их необходимо хранить в надежном месте, исключающем доступ к ним неуполномоченных лиц. Рекомендуется для хранения использовать надежные металлические хранилища.

2.3. В течение рабочего дня вне времени составления передачи и приема Электронных документов, а также по окончании рабочего дня носители ключевой информации (если Ключевая информация хранится на отдельных носителях) необходимо помещать в хранилище.

2.4. Не допускается:
- снимать несанкционированные копии с носителей ключевой информации;
- знакомить с содержанием носителей ключевой информации или передавать носители ключевой информации лицам, к ним не допущенным;
- выводить Ключи электронной подписи на дисплей компьютера или принтер;
- устанавливать носитель Ключевой информации в считывающее устройство компьютера, программные средства которого функционируют в непредусмотренных (нештатных) режимах, а также на другие компьютеры;
- записывать на носители ключевой информации постороннюю информацию.

2.5. В случае компрометации Ключей электронных подписей должна быть проведена их замена.

3. Требования по обеспечению информационной безопасности при использовании Клиентом метода аутентификации и подтверждения операций в системе ВТБ БО — Генератора паролей и EMV-карты/Программного токена.

3.1. Использование Генератора паролей и EMV-карты/Программного токена допускается в целях, определенных в настоящем Соглашении.

3.2. Использование Клиентом метода аутентификации и подтверждения операций в системе ВТБ БО с помощью Генератора паролей и EMV-карты возможно при условии наличия EMV-карты у каждого Пользователя Клиента, с помощью Программного токена возможно при условии, что пользователю Клиента подключен Программный токен в ВТБ-Онлайн.

3.3. Получение EMV-карты в офисе Банка должно осуществляться лично каждым Пользователем Клиента.

3.4. Генератор паролей и EMV-карту/Программный токен в течение рабочего дня вне времени составления передачи и приема Электронных документов, а также по окончании рабочего дня необходимо хранить в надежном месте, исключающем доступ к ним неуполномоченных лиц.

3.5. Не допускается:
- использовать в системе «ВТБ Бизнес Онлайн» Генераторы паролей, полученные вне Банка;
- подвергать Генератор паролей механическим воздействиям, приводящим к повреждению экрана, разъема для карты, порче батарейки;

- хранить ПИН вместе с EMV-картой;
- передавать EMV-карту и ПИН, Программный токен третьему лицу;
- перепривязывать EMV-карту в системе «ВТБ Бизнес Онлайн» другому пользователю Клиента;

3.6. В случае компрометации Генератора паролей / EMV-карты должна быть произведена их замена.

3.7. В случае утери мобильного устройства, на котором установлен Программный токен, немедленно отменить регистрацию Программного токена в ВТБ-Онлайн, заблокировать дистанционный доступ к ВТБ-Онлайн или отвязать от системы ВТБ БО все EMV-карты, используемые в ВТБ-Онлайн.
В случае утери мобильного устройства, на который Банк направляет SMS-коды, Клиент должен приостановить доступ к системе «ВТБ Бизнес Онлайн».

4. Требования по обеспечению информационной безопасности Мобильного устройства, с которого осуществляется работа в системе «ВТБ Бизнес Онлайн».

4.1. Устанавливайте приложение и его обновления только через официальные магазины: Google Play, Apple Store. Установка приложений из сторонних источников должна быть запрещена.

4.2. Не открывайте ссылки и SMS-сообщения на устройстве, полученные от неизвестных вам лиц.

4.3. Не «взламывайте» систему защиты вашего устройства (jailbreak\root), так как это делает его уязвимым.

4.4. Не подключайте устройство к недоверенному компьютеру.

4.5. Своевременно устанавливайте обновления операционной системы, Мобильного приложения и других приложений на вашем устройстве.

4.6. Для операционной системы Android необходимо установить антивирус для мобильного устройства и настроить его на регулярное автоматическое обновление.

4.7. Установите пароль для доступа к вашему устройству, в этом случае при утере им никто не сможет воспользоваться.

4.8. Не храните на устройстве конфиденциальную информацию (PIN-коды платежных карт, пароли для доступа к системе ВТБ-БО и т.п.).

4.9. Удаляйте конфиденциальную информацию в случае передачи мобильного устройства другим лицам (продажа устройства, передача в ремонт). Воспользуйтесь функцией восстановления заводских настроек устройства.

4.10. Подключите элементы дистанционного управления для дистанционной блокировки и дистанционного удаления данных при утрате мобильного устройства. В случае утери устройства воспользуйтесь этой функцией.

4.11. Если вы обнаружили, что ваша SIM-карта заблокирована без вашего ведома, необходимо немедленно приостановить доступ к системе «ВТБ Бизнес Онлайн», позвонив в call-центр ВТБ по телефону 8 (800) 100–24–24 или вашему менеджеру в офисе Банка.