Для аутентификации в мобильном приложении используется ПИН-код, который был назначен Вами при его активации.

3.Первоначальный экран мобильного приложения содержит только поле ввода ПИН-кода. В случае если на данном экране от Вас требуется ввод любой другой конфиденциальной информации, следует прекратить использование услуги и связаться с Банком.

4.Используйте антивирус для мобильного устройства и своевременно устанавливайте на него обновления вирусных баз.

5.В настройках безопасности мобильного устройства с операционной системой Android не рекомендуется включать пункт «Неизвестные источники».

6.Устанавливайте приложения только из официальных источников (iOS -AppStore, для Android — Play Маркет).

Помните, что Банк не рассылает своим клиентам ссылки или указания на установку приложений через СМС/ММС/E-mail — сообщения или через мессенджеры (Telegram, WhatsApp, Viber, и т.п.).

Над брошюрой работали:

Слинкова Ю.В.— специалист по социальной работе организационно-методического отделения.

(при информационной поддержке Сбербанк Онлайн)

ГБУ АО «Белогорский комплексный центр социального обслуживания населения»

Меры информационной безопасности при работе в Сбербанк Онлайн

Организационно-методическое отделение

2017 год

Несмотря на то, что банки тратят большое количество средств и сил для обеспечения безопасности своих клиентов, абсолютной защиты финансовых операций, проводимых через Интернет, не существует. Это не должно удивлять – абсолютной безопасности не бывает ни при одном типе финансовых операций. Многие клиенты банка отлично знают о мерах безопасности, которых нужно придерживаться в сфере операций с наличными, но недостаточно ознакомлены с тем, какие правила нужно знать при работе со своими данными через банковские мобильные приложения или в системе Сбербанк Онлайн. Отмахиваться от этой информации и считать ее бесполезной не имеет смысла – возврата к старым формам обслуживания не будет и через несколько лет почти все банковские операции будут проводиться без походов в банк в любое время суток. Чем быстрее гражданин поймет и выучит не такие уж сложные правила безопасности работы в отдаленном доступе, тем удобнее будет его жизнь и целее деньги на счетах.

Рекомендации для клиентов, использующих VPN KEY TLS

Используйте токен VPN KEY TLS только в период работы в СББОЛ, после окончания отключайте их от компьютера.

Требования к хранению ПИН-кодов VPN KEY TLS токен аналогичны требованиям к хранению ПИН-кодов банковских карт: никто кроме Вас не должен знать ПИН-код.

Выполняйте незамедлительную блокировку и смену ключей электронной подписи (далее — ЭП) в случаях их компрометации, а так же по истечению срока действия ключей с периодичностью, установленной договорами и документацией.

4. Заменяйте ключи ЭП во всех случаях увольнения или смены руководителей юридического лица, которые подписывали распоряжения (доверенность) о предоставлении полномочий по подписи электронных документов ЭП, а также при любом подозрении на компрометацию ключа ЭП.

Рекомендации для клиентов, использующих Мобильное приложение

1. Установите парольную защиту на Вашем мобильном устройстве. Данная возможность доступна для любых современных моделей планшетов/телефонов.

2. Не вводите в мобильном приложении или где-либо еще Ваш пароль к полнофункциональной версии СББОЛ, мобильное приложение его не использует.

Используйте проверенные программы

Для того, чтобы не допустить утечку личных данных, пользуйтесь мобильными приложениями, разработанными Сбербанком для своих клиентов. Скачать их можно из официальных магазинов приложений в зависимости от программного обеспечения, установленного на гаджете. Не следует устанавливать на смартфонах сторонние браузеры, переходить на незнакомые ресурсы или открывать сомнительные ссылки – возможно, это вирус, который создан для кражи данных. Необходимо установить на гаджете современное качественное антивирусное программное обеспечение и регулярно его обновлять.

Рекомендации для клиентов с СМС-паролем

Не пользуйтесь СББОЛ в браузере того же мобильного устройства, на которое приходят СМС-сообщения с подтверждающим одноразовым паролем.

2. При утрате мобильного телефона, на который Банк отправляет СМС-сообщения с подтверждающим одноразовым паролем, следует оперативно обратиться к своему оператору сотовой связи для блокировки абонентского номера и замены СИМ-карты, а также обратиться в Банк для выявления возможных несанкционированных операций.

Что нужно знать, работая с банком через гаджеты

В современном мире информация приравнивается к деньгам. Знание личной информации о клиенте даст возможность мошенникам похитить его средства. Часто человек, не придавая значения элементарным правилам безопасности, становится жертвой мошенников в ситуации, которую спровоцировал сам. Рекомендации банка по мерах безопасности для своих клиентов обязательны к выполнению – за ними стоит опыт пострадавших. При нарушении этих правил клиент не только не сможет вернуть свои средства, но и предъявить кому-либо претензии по поводу утраты денег.

Пароли –личная информация

Пароль, логин, ПИН– личные данные каждого пользователя банковских программ и продуктов. Это как ключ от квартиры, который не дают кому попало и тем более не кладут под половичок под дверью. Эти данные не сообщаются никому, не пишутся на бумажке и не лепятся на стикере к монитору компьютера. Если была необходимость в посторонней помощи в выполнении какой-либо операции с логином и паролем доступа на чужом компьютере – поменяйте пароль в тот же день. Не пишите ПИН на обороте карт или на приклеенной к карте бумажке, если нужно было кому-то сообщить ПИН – поменяйте его в тот же день. ПИН не нужен сотрудникам банка для обслуживания клиентов, им также не

нужны большинство его личных данных, но они нужны мошенникам для того, чтобы украсть чужие деньги. Будьте внимательны!

Меры информационной безопасности при работе в Сбербанк Бизнес Онлайн

Логин, пароль, ПИН-код для токена VPN KEY TLS, одноразовые СМС-пароли, кодовое слово — это Ваша личная конфиденциальная информация, ни при каких обстоятельствах не раскрывайте их никому, включая сотрудников Сбербанка России (далее — Банк). При обращении к Вам с любыми просьбами сообщить конфиденциальную информацию не делайте этого, перезвоните в контактный центр Банка.

Первоначальная страница доступа в личный кабинет содержит только поля ввода логина и пароля. В случае, если на данной странице от Вас требуется ввод любой другой персональной информации (номеров банковских карт, мобильного телефона и других личных данных), следует прекратить пользование услугой и обратиться в Банк по номерам, указанным на официальном сайте Банка.

При обнаружении Вами попыток несанкционированного доступа или в случае мотивированных опасений, что такие попытки могут быть, рекомендуется незамедлительно сообщить об этом Банку по телефону или обратиться к Вашему клиентскому менеджеру в ВСП.

4. При подтверждении операций одноразовым СМС-паролем необходимо контролировать соответствие реквизитов операции и реквизитов в полученном

СМС-сообщении (проверяйте ИНН и номер счета, не ограничивайтесь проверкой совпадения только наименования получателя платежа).

5. При работе в Сбербанк Бизнес Онлайн (далее — СББОЛ) убедитесь, что защищенное ssl-соединение установлено именно с официальным сайтом услуги (https://sbi.sberbank.ru:9443/ic), настоятельно не рекомендуется переходить на данную страницу по ссылке с Интернет-ресурсов (за исключением официальных ресурсов банка, например, www.sberbank.ru).

Внимание! Для дополнительной защиты в ряде случаев сотрудники Банка могут позвонить Вам и попросить подтвердить легитимность операций. Сотрудник Банка может запросить номер платежного поручения, пять последних цифр счёта получателя, сумму и название компании, на которую осуществляется платёж.

Обращаем внимание, что звонки из контактных центров Банка могут поступать с номеров:

+7 (383) 319-38-41, +7 (383) 319-25-09, +7 (383) 319-25-48, +7 (383) 319-24-39, +7 (383) 319-32-99, +7 (383) 319-26-43, +7 (383) 319-31-88, +7 (383) 319-30-96, +7 (383) 319-33-88, +7 (383) 319-26-46, +7 (383) 319-32-24, +7 (383) 319-32-62, +7 (383) 319-30-14, +7 (383) 319-26-64, +7 (383) 319-24-48, +7 (383) 319-24-14, +7 (383) 319-32-15, +7 (383) 319-33-34, +7 (383) 319-30-75, +7 (383) 319-38-66