Приложение №2
к Правилам дистанционного банковского обслуживания АО «ГУТА-БАНК» клиентов-физических лиц с использованием Системы дистанционного банковского обслуживания «ГУТА-БАНК»

ГУТА БАНК

Рекомендации клиентам по обеспечению необходимого уровня информационной безопасности при работе в Системе дистанционного банковского обслуживания «ГУТА-БАНК»

Соблюдение настоящих рекомендаций, направленных на обеспечение информационной безопасности и предотвращение мошенничества при использовании Системы ДБО, позволит обеспечить защиту конфиденциальной информации, а также снизит возможные риски при совершении Операций в Системе.

Банк не несет ответственности перед Клиентом за ущерб, полученный Клиентом в результате несоблюдения рекомендаций, предусмотренных настоящим документом.

Все термины, указанные в настоящем документе, используются в значении, определенном в Правилах дистанционного банковского обслуживания АО «ГУТА-БАНК» клиентов-физических лиц с использованием Системы дистанционного банковского обслуживания «ГУТА-БАНК».

1. Обеспечение безопасности компьютера и/или мобильного устройства, с использованием которого осуществляется работа в Системе:

1. Устанавливайте и запускайте только лицензионное программное обеспечение (операционная система, браузер, офисные программы и т.д.).
2. Настоятельно рекомендуем устанавливать на компьютере/мобильном устройстве лицензионное антивирусное программное обеспечение. Регулярно производите его обновление и полную антивирусную проверку компьютера/мобильного устройства, а также обновление операционной системы и используемых программ (браузера и иных программ). Используйте программное обеспечение только из проверенных и надежных источников.
3. Для предотвращения несанкционированного доступа по сети к компьютеру, с которого осуществляется работа в Системе, по возможности, необходимо установить и настроить персональный брандмауэр (firewall).

2. При работе в Системе необходимо придерживаться следующих правил:

1. Осуществляйте вход и работу в Системе только с личного компьютера/мобильного устройства. Категорически не рекомендуется работать с Системой в местах с общедоступных компьютеров, не заслуживающих доверия (интернет-кафе, чужой компьютер и т.п.) или с использованием общественных каналов связи (бесплатный Wi-Fi и т.п.), т.к. это существенно увеличивает риск кражи Ваших персональных данных.
2. Не храните на мобильном устройстве и/или компьютере конфиденциальную информацию о Вашем Логине и Пароле для доступа к Системе в виде, не защищенном от доступа третьих

лиц. Не используйте функцию автозаполнения в установках браузера, это позволит не сохранять данные (Пароль, Логин и др.) в памяти браузера, что, в свою очередь, предотвратит использование данных сторонними лицами. После окончания работы в Системе, очищайте кэш браузера.

3. Удаляйте конфиденциальную информацию в случае передачи мобильного устройства и/или компьютера другим лицам (продажа устройства, передача в ремонт и т.п.).

4. После окончания работы в Системе обязательно завершайте сеанс, используя кнопку «Выход».

5. Поставьте пароль на вход в ваш профиль на компьютере и обязательное условие ввода пароля для входа после отключения «спящего режима», используйте функцию блокировки мобильного устройства. Наиболее надежным методом блокировки мобильных устройств является сканер отпечатков пальцев. Если на устройстве нет такой возможности, обязательно используйте защиту с помощью пароля или графического ключа.

6. Используйте достаточно сложный Пароль для входа в Систему. Пароль должен иметь длину не менее 8 (Восьми) символов, содержать хотя бы по одному символу из заглавных и прописных букв латинского алфавита (a-Z, A-z), а также цифры (0-9). Пароль не должен содержать последовательности одинаковых символов, персональную информацию (имена и даты рождения членов семьи, номера телефонов и т.п.). Пароль не должен являться копией других паролей, используемых в личных целях (на развлекательных и почтовых сайтах в Интернете).

7. Производите смену Пароля не реже одного раза в месяц. Новое значение Пароля не должно совпадать с предыдущими Паролями на протяжении пяти смен.

8. При самостоятельной смене Логина в Системе устанавливайте достаточно сложный Логин. Логин должен иметь длину не менее 8 (Восьми) символов, содержать прописные буквы латинского алфавита (a-z) и цифры (0-9).

9. Избегайте присутствия третьих лиц при осуществлении Самостоятельной регистрации в Системе, смене Логина и Пароля.

10. Контролируйте посещения Системы. Проверяйте дату Вашего последнего посещения и IP-адрес (данная информация отображается в разделе «Сервис» - «Пользовательская активность»).

11. Исключите посещение с мобильного устройства и/или компьютера сайтов сомнительного содержания.

12. При входе в Систему убедитесь в безопасности соединения, включая наличие символа замка в левом верхнем углу в адресной строке браузера. Его наличие означает, что соединение с Системой защищено по протоколу SSL.

Осуществляйте вход только убедившись, что в адресной строке web-браузера используется защищенный протокол HTTPS, т.е. адресная строка в браузере начинается с https://.

13. Никогда не следует переходить на страницу Системы по ссылкам с интернет-ресурсов, за исключением официального сайта www.gutabank.ru, по ссылкам из поступивших по электронной почте писем или по ссылкам из средств мгновенного обмена сообщениями.

14. Ни при каких обстоятельствах никому, включая сотрудников Банка, не раскрывайте личную конфиденциальную информацию.

15. Не сообщайте в ответ на телефонные звонки, СМС-сообщения или сообщения по электронной почте, поступившие якобы от работников Банка, Средства доступа к Системе. Не перезванивайте в ответ на подобные звонки. Для обращения в Банк используйте официальные телефоны, указанные на сайте Банка.

16. Не выполняйте никакие рекомендации, особенно связанные с вводом каких-либо данных на любых страницах, открытых браузером в интернете. Следует иметь в виду, что работники

Банка никогда не обращаются к Клиентам по телефону с предложениями попытаться войти в Систему еще раз или ввести еще один Код подтверждения, не пытаются узнать у Клиентов Средства доступа к Системе или реквизиты Карты.

Примечание: При обращении в ЦКП, сотрудники ЦКП в целях Идентификации Клиента запрашивают Фамилию, Имя, Отчество, Логин, Кодовое слово и номер Карты Клиента. НИКАКИХ ДРУГИХ ДАННЫХ сотрудники ЦКП не запрашивают.

17. При получении СМС-сообщения обращайте внимание на отправителя. Банк отправляет СМС-сообщения от имени абонента – GUTABANK.
18. Старайтесь избегать регистрации Номера мобильного телефона в социальных сетях и других открытых и доступных источниках.
19. В случае внезапного приостановления работы SIM-карты, связанной с Номером мобильного телефона, незамедлительно обратитесь к оператору мобильной связи для выяснения причин блокировки. В случае необходимости, обратитесь в ЦКП с целью блокировки доступа к Системе.
20. При смене Номера мобильного телефона обратитесь в ЦКП или Офис Банка.
21. Вводите Код подтверждения только в том случае, если Операция инициирована Вами. При получении СМС-сообщения с Кодом подтверждения внимательно ознакомьтесь с его содержанием, проверьте детали и содержание Операции, которую Вы подтверждаете Кодом подтверждения. Вводить Код подтверждения в Систему следует только тогда, когда реквизиты и детали Вашей Операции в Системе соответствуют реквизитам в полученном СМС-сообщении.
22. Если при входе в Систему замечены какие-либо несоответствия стандартным запросам или поступают от имени Банка звонки с предложением попытаться войти в Систему еще раз, ввести или сообщить Средства доступа к Системе, незамедлительно обратитесь в ЦКП по телефонам, указанным ниже, не совершая никаких действий.

3. Рекомендации по использованию Мобильного Банка «ГУТА-БАНК»

1. Устанавливайте приложение Мобильного Банка «ГУТА-БАНК» и его обновления только из приложений Apple AppStore / Google Play Market. Ссылки для установки указаны на сайте Банка www.gutabank.ru.

В случае установки приложения из других источников Клиент несет риски использования Системы, связанные с возможным нарушением безопасности и возможным получением несанкционированного доступа к защищенной информации.

Банк не рассылает своим Клиентам ссылки или указания на установку приложений через СМС/E-mail – сообщения.

2. Если на мобильном устройстве реализована поддержка технологий Touch ID и Android Fingerprint Authentication (датчик отпечатка пальца), используйте ее для разблокировки и Аутентификации в Мобильном Банке «ГУТА-БАНК».
3. Не «взламывайте» систему защиты iPhone (jailbreak) и не открывайте «root» доступ для устройств на операционной системе Android, так как это делает уязвимым Ваше мобильное устройство.
4. Подключите элементы дистанционного управления (для дистанционной блокировки и дистанционного удаления данных с мобильного устройства при утрате мобильного устройства).
5. Не подключайте мобильное устройство к устройствам, безопасность которых Вы не можете гарантировать.

6. При утрате мобильного телефона (иного устройства), на который направляются Коды подтверждения или на которое установлен Мобильный Банк «ГУТА-БАНК», незамедлительно обратитесь в ЦКП для блокировки доступа к Системе.

При возникновении подозрений в осуществлении несанкционированных Операций в Системе либо при Компрометации Средств доступа необходимо выполнить следующие действия:

1. Незамедлительно обратиться в Банк для блокировки доступа к Системе. Это можно сделать по звонку в ЦКП, а также в Офисе Банка.
2. Возобновление доступа к Системе, смена Логина производятся в Офисе Банка при личном обращении Клиента.

О появлении несанкционированных действий в Системе, требующих незамедлительного обращения в Банк, могут свидетельствовать следующие факты:

- В истории операций в Системе указаны Распоряжения, которые Вы не создавали.
- Подозрительная активность на компьютере, с которого осуществляется работа с Системой (открытие или закрытие окон, движение курсора мыши и т.п.).
- Осуществлен запрос на ввод Кода подтверждения для повторного подтверждения входа в Систему, подтверждения смены Логина или Пароля, подтверждения Распоряжения, которое Вы не создавали.
- Перенаправление на другой сайт при подключении к Системе, изменение адреса в адресной строке браузера при работе с Системой.
- Получение сообщения о блокировке или разблокировке доступа в Систему.
- Наличие в истории входов в Систему информации о входе в Систему с незнакомого IP-адреса.
- Невозможность получения доступа к Системе по причине несовпадения Пароля при введении заведомо верного Пароля.
- Внезапное приостановление работы SIM-карты, на номер которой посредством СМС-сообщений направляются Коды подтверждения.
- Изменение интерфейса Системы без предварительного уведомления на сайте Банка о вносимых в Систему изменениях.
- Подозрительная работа (зависание, самопроизвольные рассылки СМС-сообщений, звонки, скачивание и загрузка приложений) мобильного устройства, с которого осуществляется работа с Системой.

Внимание! По всем вопросам, связанным с дистанционным обслуживанием, Вы можете обратиться в Центр Клиентской поддержки Банка по телефонам:

- +7 495 771 74 44;
- 8 800 100 47 00 (звонок по России бесплатный).

Адрес электронной почты для направления вопросов и обращений, связанных с дистанционным обслуживанием: Client@gutabank.ru.