

Политика конфиденциальности мобильного приложения «Сбербанк Онлайн»

Настоящая Политика конфиденциальности (далее — Политика) мобильного приложения «Сбербанк Онлайн» (далее — Приложение) действует в отношении той информации, которую ПАО Сбербанк (далее – Банк) может получить с устройства пользователя во время использования им Приложения.

Использование Приложения означает безоговорочное согласие пользователя с настоящей Политикой и указанными в ней условиями обработки информации, получаемой с устройства пользователя. В случае несогласия с Политикой пользователь должен воздержаться от использования Приложения.

Приложение и услуги в рамках Приложения реализуются пользователю на основании договоров и соглашений с Банком, которые в числе прочего регулируют все вопросы обработки и хранения Банком персональных данных пользователя.

Настоящая Политика применима только к Приложению. Банк не контролирует и не несет ответственность за информацию (последствия её передачи), переданную пользователем третьей стороне, в случае если такая передача была выполнена на ресурсе третьей стороны, на который пользователь мог перейти по ссылкам из Приложения.

Банк имеет право вносить изменения в настоящую Политику путем размещения новой редакции Политики на сайте Банка и/или в Приложении. Обязанность самостоятельного ознакомления с актуальной редакцией Политики лежит на пользователе.

1. Состав информации, которая может быть получена с устройства пользователя при использовании Приложения и цели её получения (далее - Информация пользователя):

1.1. Информация о номерах телефонов из адресной книги устройства.

Цель: номера телефонов из адресной книги контактов на устройстве пользователя используются в Приложении для облегчения совершения пользователями операций переводов денежных средств.

При установке Приложения пользователь дополнительно информируется о целях использования в Приложении данных о номерах телефонов из его адресной книги.

При использовании в Приложении данные о номерах телефонов копируются на серверы Банка и могут периодически обновляться.

1.2. Информация о местоположении устройства пользователя (на основе данных сети оператора сотовой связи и сигналов GPS)

Цель: информирование пользователя при использовании Приложения о местоположении подразделений Банка и устройств самообслуживания Банка, а также о дополнительных сервисах, доступных пользователю и обусловленных его местоположением.

1.3. Фотоизображения, полученные с использованием камеры устройства.

Цель: получение и использование фотоизображений в рамках услуг, реализуемых в Приложении, в том числе для создания и сохранения фотоизображений в профиле пользователя в Приложении, получения фотоизображений платежных документов и штрих-кодов с целью их распознавания и использования для совершения операций по переводу денежных средств в Приложении.

1.4. Информация о версии операционной системы и модели устройства.

Цель: анализ возможных ошибок в работе Приложения и совершенствование работы Приложения.

Для целей анализа Банк может передавать информацию об операционной системе и модели устройства сторонним организациям в обезличенном виде.

1.5. Информация об IP-адресе и адресе точки подключения пользователя.

Цель: повышение безопасности пользователя при использовании Приложения и совершения финансовых операций.

1.6. Информация об SMS-сообщениях на устройстве Пользователя.

Цель: сохранение и использование в Приложении SMS-сообщений, поступивших от Банка (с номера 900).

1.7. Аудиоданные, полученные с использованием микрофона устройства (реализуется в Приложении при наличии технической возможности)

Цель: выполнение аудио звонков пользователя в Банк с использованием Приложения.

1.8. Использование встроенного в Приложение антивируса.

1.8.1. Цель: повышение уровня оперативной защиты:

- информация об установленном ПО, в том числе уникальный идентификатор установки ПО на устройстве, идентификатор и версия используемого ПО, уникальный идентификатор устройства, уникальный идентификатор пользователя в сервисах правообладателя;
- информация о проверяемых URL, в том числе URL, по которому запрашивается репутация, и URL страницы, с которой был получен проверяемый URL, идентификатор протокола соединения и номер используемого порта;
- информация о проверяемых сертификатах, в том числе URL и IP адреса сайта, для которого осуществляется проверка, серийный номер и содержимое проверяемого сертификата, а также его тип и контрольная сумма (MD5);
- информация для получения репутации проверяемого файла, в том числе его контрольная сумма (MD5), а также тип детектирования, идентификатор использованной записи в базе угроз, тип и время создания записи;

1.8.2. Цель: выявление новых и сложных для обнаружения угроз информационной безопасности и их источников, угроз вторжения, а также повышения уровня защиты информации, хранимой и обрабатываемой пользователем на устройстве:

- информация об установленном ПО, в том числе уникальный идентификатор установки ПО на устройстве, идентификатор и версия используемого ПО, уникальный идентификатор устройства, данные о типе устройства и установленной на нем ОС и пакетов обновлений ОС;
- информация об атаках, связанных с подменой сетевых ресурсов, в том числе URL, на котором обнаружена подмена, версия используемой базы угроз, идентификатор записи в базе, соответствующий обнаруженной угрозе, имя, контрольная сумма (MD5) и размер файла приложения, запросившего подмененный URL, тип клиента, весовой уровень атаки, название цели атаки, уровень надежности обнаружения, признак Silent-детектирования;
- информация о проверенных файлах, в том числе название файла и контрольная сумма (MD5), путь к нему и код шаблона пути, код и идентификатор типа файла, признак исполняемого файла, название обнаруженной угрозы согласно классификации правообладателя, время выпуска и время последнего обновления антивирусной базы, идентификатор и тип использованной записи в базе, признак отладочного детектирования, идентификатор уязвимости и класс её опасности, идентификатор задачи ПО, в рамках которой выполнена проверка, признак проверки или подписи файла.

1.8.3. Цель: улучшение качества работы ПО и обновления ПО:

- информация о результатах обновления ПО, в том числе тип и уникальный идентификатор устройства, на котором установлено ПО, уникальный идентификатор установки ПО на устройстве, идентификаторы ПО и задачи обновления, идентификатор и версия обновления ПО, идентификатор настроек обновления ПО, результат

обновления ПО, идентификатор условия формирования передаваемой статистики, идентификатор настроек ПО, идентификатор и название партнера, для которого выпущено ПО, язык локализации ПО, уникальный идентификатор и тип установленной лицензии, данные об установленной ОС, в том числе тип и версия, идентификатор программы «приведи друга», доступной для ПО;

- информация о возникших ошибках в работе компонент ПО, в том числе тип и время возникновения ошибки, а также идентификатор компонента ПО и задачи, при выполнении которой возникла ошибка, копия участка оперативной памяти устройства, относящегося к вызвавшему ошибку компоненту ПО, тип и время создания копии участка оперативной памяти, даты создания, активации и истечения используемого лицензионного ключа, количество компьютеров, на которое рассчитана лицензия, имя первичного файла обновления, дата и время первичных файлов предыдущего и нового обновлений, дата и время завершения последнего обновления, версия набора передаваемой информации, время отправки информации.

1.8.4. Цель: защита пользователя от мошенничества при посещении страниц сайта Банка:

- Идентификатор и версию используемого ПО, уникальный идентификатор компьютера, информацию о состоянии используемого браузера, идентификатор параметров настроек ПО.

1.8.5. Цель: повышение уровня защиты информации, хранимой и обрабатываемой пользователем на устройстве:

- Идентификатор и версия используемого ПО, уникальный идентификатор устройства, тип и версия установленной ОС, тип и версия браузера, время последнего обновления антивирусных баз;
- информация об атаках, связанных с подменой сетевых ресурсов, в том числе URL, на котором обнаружена подмена, название цели и метода обнаружения атаки;
- информация о проверяемых сертификатах, в том числе URL и IP адресе сайта, для которого осуществляется проверка, контрольная сумма (MD5) проверяемого сертификата, причина его не действительности;
- информация об обнаруженных угрозах и уязвимостях, в том числе название угрозы и результат ее устранения, признак обнаружения уязвимости ОС, идентификатор угрозы, обнаруженный при запуске браузера, признак обнаружения загрузки не доверенного модуля;
- информация об уровне защиты от получения снимков экрана

Указанные выше данные по встроенному антивирусу могут также использоваться для формирования отчетов по рискам информационной безопасности.

Дополнительно в рамках настоящей Политики Банк вправе использовать дополнительные программные инструменты (в том числе партнеров Банка) и cookies для сбора и обработки обезличенной статистической информации об использовании пользователем Приложения и услуг в рамках Приложения для целей улучшения Приложения;

2. Условия обработки Информации пользователя

- 2.1. В соответствии с настоящей Политикой Банк осуществляет обработку только той информации и только для тех целей, которые определены в пункте 1.
- 2.2. Встроенный в Приложение антивирус обрабатывает полученную информацию, исключая данные, относящие к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), и никак не связывает обрабатываемую информацию с персональными данными пользователя.

- 2.3. Банк принимает все зависящие от Банка организационные и технические меры для защиты Информации пользователя от неправомерного доступа третьих лиц, использования, копирования и распространения.
- 2.4. Для целей, изложенных в настоящей Политике, Банк может привлекать к обработке Информации пользователя партнеров, с которыми у Банка заключены соответствующие соглашения о конфиденциальности. Передача Банком партнерам обезличенных данных об использовании Приложения для целей улучшения работы Приложения осуществляется на основании договоров с партнерами.
- 2.5. Информация пользователя может сохраняться на ресурсах Банка и его партнеров в течение срока действия договорных отношений между Банком и пользователем касаясь Приложения, а также в течение 5 лет после расторжения таких договоров.
- 2.6. Информация Пользователя может быть предоставлена государственным органам в соответствии с требованиями действующего законодательства.