

Политика конфиденциальности Мобильного приложения «СберKids»

Настоящая Политика конфиденциальности Мобильного приложения «СберKids» (далее - Политика) действует в отношении той информации, которую Банк может получить с Устройства Пользователя во время использования им МП «СберKids».

1. Термины и определения

1.1. **Банк** – лицензиар, Публичное акционерное общество «Сбербанк России» ПАО Сбербанк ИНН 7707083893, КПП 775001001, р/с 30301810000006000001, к/с 30101810400000000225, БИК 044525225, ОКВЭД 65.12, ОКПО, 00032537, ОГРН 1027700132195.

1.2. **Мобильное приложение «СберKids» (далее – МП «СберKids»)** - программное обеспечение для мобильных устройств на базе операционных систем¹ iOS и Android, предназначенное для управления ПВК Пользователем и Малолетним пользователем, предоставляющее Пользователю возможность доступа к РК «СберKids», а Малолетнему пользователю - к ДК «СберKids».

1.3. **Пользователь** – лицензиат, физическое лицо, законный представитель Малолетнего пользователя, зарегистрированный в МП «СберKids».

1.4. **Сайт Банка** – сайт Банка в сети интернет по адресу: www.sberbank.ru, на котором размещена информация по МП «СберKids».

1.5. **Устройство** – мобильное техническое устройство Пользователя, Малолетнего пользователя (смартфон, планшет или другое устройство), имеющее доступ к сети Интернет, на котором установлено МП «СберKids».

2. Общие положения

1.1. Использование МП «СберKids» означает безоговорочное согласие Пользователя с настоящей Политикой и указанными в ней условиями обработки информации, получаемой с Устройства. В случае несогласия с Политикой Пользователь должен воздержаться от использования МП «СберKids».

1.2. Услуги в рамках МП «СберKids» реализуются Пользователю на основании договоров и соглашений с Банком, которые в числе прочего регулируют все вопросы обработки и хранения Банком персональных данных Пользователя.

1.3. Настоящая Политика применима только к МП «СберKids». 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 МП «СберKids».

¹ версии: iOS 8.3. - и новее, Android 5.1. - и новее

1.4. Банк имеет право вносить изменения в настоящую Политику путем размещения новой редакции Политики на Сайте Банка и/или в МП «СберKids». Обязанность самостоятельного ознакомления с актуальной редакцией Политики лежит на Пользователе.

3. Состав информации, которая может быть получена с Устройства при использовании МП «СберKids» и цели её получения

3.1. Фотофайлы, полученные с использованием камеры Устройства.

Цель: получение и использование фотоизображений в рамках услуг, реализуемых в МП «СберKids», в том числе для создания и сохранения фотоизображений в профиле Пользователя.

3.2. Информация о версии операционной системы и модели Устройства.

Цель: анализ возможных ошибок в работе МП «СберKids» и совершенствование работы МП «СберKids».

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

3.3. Информация о пройденных опросах от исследовательских компаний с ответами, выбранными Пользователем.

3.4. Информация раздела желаний МП «СберKids», в том числе ссылки и фотографии, размещенные в данном разделе.

Цель: предоставление услуг, реализуемых в рамках МП «СберKids».

3.5. Использование встроенной в МП «СберKids» антивирусной программы.

1 Цель: повышение уровня оперативной защиты:

- информация об установленном программном обеспечении, в том числе уникальный идентификатор установки программного обеспечения на Устройстве, идентификатор и версия используемого программного обеспечения, 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.

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 программном обеспечении, в том числе уникальный идентификатор установки программного обеспечения на Устройстве, идентификатор и версия используемого программного обеспечения, уникальный идентификатор Устройства, данные о типе Устройства и установленной на нем операционной системы и пакетов обновлений операционной системы;
- 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 программного обеспечения, в рамках которой выполнена проверка, признак проверки или подписи файла.

3 Цель: улучшение качества работы программного обеспечения и обновления программного обеспечения:

- информация о результатах обновления программного обеспечения, в том числе тип и уникальный идентификатор Устройства, на котором установлено программное обеспечение, уникальный идентификатор установки программного обеспечения на Устройстве, идентификаторы программного обеспечения и задачи обновления, идентификатор и версия обновления программного обеспечения, идентификатор настроек обновления программного обеспечения, результат обновления программного обеспечения, идентификатор условия формирования передаваемой статистики, идентификатор настроек программного обеспечения, идентификатор и название партнера, для которого выпущено программное обеспечение, язык локализации программного обеспечения, уникальный идентификатор и тип установленной лицензии, данные об установленной операционной системы, в том числе тип и версия, идентификатор программы «приведи друга», доступной для программного обеспечения;
- информация о возникших ошибках в работе компонент программного обеспечения, в том числе тип и время возникновения ошибки, а также идентификатор компонента программного

обеспечения и задачи, при выполнении которой возникла ошибка, копия участка оперативной памяти Устройства, относящегося к вызвавшему ошибку компоненту программного обеспечения, 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.

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.

4 Цель: повышение уровня защиты информации, хранимой и обрабатываемой пользователем на Устройстве:

- Идентификатор и версия используемого программного обеспечения, уникальный идентификатор Устройства, тип и версия установленной операционной системы, 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 операционной системы, 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.

4. Условия обработки информации Пользователя

4.1. В соответствии с настоящей Политикой Банк осуществляет обработку только той информации и только для тех целей, которые определены в п.3. настоящей Политики.

4.2. Встроенный в МП «СберKids» 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.

4.3. Банк принимает все зависящие от Банка организационные и технические меры для защиты информации Пользователя от неправомерного доступа третьих лиц, использования, копирования и распространения.

4.4. 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 МП «СберKids» для целей улучшения работы МП «СберKids» осуществляется на основании договоров с партнерами.

4.5. Информация Пользователя может сохраняться на ресурсах Банка и его партнера в течение срока действия договорных отношений между Банком и Пользователем касаясь МП «СберKids», а также в течение 5 лет после расторжения таких договоров.

4.6. Информация Пользователя может быть предоставлена государственным органам в соответствии с требованиями действующего законодательства РФ.