Руководство пользователя LATEBRA

ВВЕДЕНИЕ

Сейчас, когда защита частной жизни и личных данных становится все более насущной проблемой, самое время задуматься о том, как реально это осуществить.
Latebra решит эти проблемы и сохранит в тайне, как вашу переписку, так и контактные данные.
Во-первых, Latebra создает изолированную «экосистему», где только акцептованные лица (избранные) могут обмениваться конфиденциальной корреспонденцией.
Во-вторых, Latebra обеспечивает шифрование Вашей корреспонденции, используя оригинальные алгоритмы, что даст Вам, если не 100% гарантию конфиденциальности, то, по крайней мере, значительно приблизит Вас к этому идеалу. Если Вы используете Latebra, никто без крипто-ключа не сможет прочитать Ваши сообщения (SMS, MMS, Email), даже если осуществит их перехват или взломает Ваш почтовый ящик.
В-третьих, Latebra защищает данные, хранящиеся в «Контактах», от несанкционированного доступа, даже если Ваше мобильное устройство (смартфон или планшет) окажется у третьих лиц.

1 ПЕРВИЧНЫЕ УСТАНОВКИ

1.1 ГЕНЕРАЦИЯ КРИПТО-КЛЮЧА ПРИЛОЖЕНИЯ

Работа с Latebra начинается с генерации крипто-ключа Приложения, который обеспечивает доступ в Latebra и будет использован для шифрования/дешифрования контактных данных. Для генерации крипто-ключа Приложения необходимо определить используемые алфавиты, установить требуемый уровень защиты, придумать и ввести кодовое слово. Эти параметры определяют крипто-ключ и его длину, например, при параметрах, приведенных на Рисунке 1.1, был сгенерирован крипто-ключ большой длины **gOndhW8Z5rUOqxqzWH**.
Легко можно посчитать, сколько комбинаций нужно перебрать, чтобы подобрать подобный ключ.

Рис. 1.1 Генерация крипто-ключа

1.1.1 ИСПОЛЬЗУЕМЫЕ АЛФАВИТЫ

По умолчанию, алгоритм шифрования Latebra предназначен для английского языка и языка локализации мобильного устройства (смартфон или планшет). Если Вы используете контактные данные на других языках, Вам нужно расширить список используемых языков, отметив соответствующие чек-боксы. В противном случае, буквы, которые Вы применяли при записи контактных данных, и которые отсутствуют в отмеченных алфавитах, не будут зашифровываться, что снизит уровень криптозащиты.

1.1.2 УРОВЕНЬ ЗАЩИТЫ

Существует возможность управления уровнем криптозащиты, которая определяется в %. Изменение уровня защиты осуществляется с помощью перемещения ползунка. Чем выше уровень защиты будет установлен, тем больше будет криптобезопасность, но тем медленнее будет происходить процесс шифрования/дешифрования. 99% соответствует максимальному уровню защиты в Latebra.

1.1.3 КОДОВОЕ СЛОВО

При генерации крипто-ключа Приложения необходимо ввести кодовое слово. Это слово будет паролем для входа в «экосистему» Latebra и его нужно запомнить. Кодовое слово обеспечивает персонификацию крипто-ключей. Чем более длинное слово будет введено, тем более длинный крипто-ключ будет сгенерирован. Кодовое слово должно содержать исключительно латинские буквы без диакритики и цифры, но последний символ не может быть цифровым Максимальная длина кодового слова ограничена 10 символами.

Кодовое слово обеспечит не только доступ в приложение, но и поможет восстановить крипто-ключ, поэтому при замене крипто-ключа Приложения желательно запомнить старое кодовое слово, оно необходимо, если понадобится дешифровать те данные, которые Вы забыли дешифровать перед заменой крипто-ключа Приложения.

.

1.1.4 КРИПТО КЛЮЧ ПРИЛОЖЕНИЯ

После выбора используемых алфавитов, определения уровня защиты, ввода кодового слова и клика кнопки крипто ключ Приложения будет сгенерирован. После генерации крипто-ключа Приложения необходимо определить режим использования кодового слова, а именно запрашивать его при каждом входе в Приложение или нет.

Рис. 1.2 Режим использования кодового слова

!!!! Мы рекомендуем установить требование ввода кодового слова при каждом старте Latebra. (А также, выходить из приложения каждый раз по завершению сеанса использования).

1.2 ПОДКЛЮЧЕНИЕ АККАУНТА

После генерации крипто-ключа Приложения желательно подключить Ваши E-mail аккаунты к Latebra. Это обеспечит возможность удобной работы с Email сообщениями, тогда Latebra будет использоваться как Email клиент с функцией шифрования/дешифрования.

Для подключения необходимо ввести E-mail адрес, пароль, кликнуть «+» и в заключение . После этого Latebra можно будет использовать как E-mail клиент.

В настоящий момент, поддерживается работа с почтовыми сервисами: Gmail и Yandex. С другими E-mail сервисами придется работать в режиме copy&paste. В дальнейшем планируется расширить список поддерживаемых сервисов.

Если Email аккаунты не подключать, то в Latebra непосредственно можно будет работать только с SMS/MMS сообщениями, а с Email придётся работать исключительно методом copy&paste.

Первичные установки всегда можно поменять в «Настройке» . На этом первичные установки завершены.

Рис 1.3 Диалог подключения аккаунта

1.3 ОСНОВНОЕ ОКНО

Рис 1.4 Основное окно

После того, как крипто-ключ Приложения создан и почтовый аккаунт(ы) подключен (опционально), то это значит, что первичная настройка Latebra завершена и можно приступить к работе с Latebra.

При дальнейшей работе с Latebra все управление осуществляется через основное окно Рис 1.4, обеспечивающее:

- Вызов «Адресной книги» для генерации и рассылки, персональных крипто ключей и работы с контактными данными, включая их шифрование; клик по кнопке «Контакты» ;
- Вызов общего клиента для загрузки сообщения всех типов (Email, SMS/MMS)в Latebra и последующих действия с ними: создание, шифрование и отсылка новых сообщений, а также просмотр списков, дешифрование и чтение полученных сообщений; клик по кнопке «Сообщения» ;
- Быстрый вызов «Редактора» для обеспечения ускорения подготовки, шифрования и отсылки сообщений без предварительной загрузки полученных сообщений; клик по кнопке «Редактор» ;
- Настройку Latebra; клик по кнопке «Настройки» .

2 РАБОТА С КОНТАКТАМИ

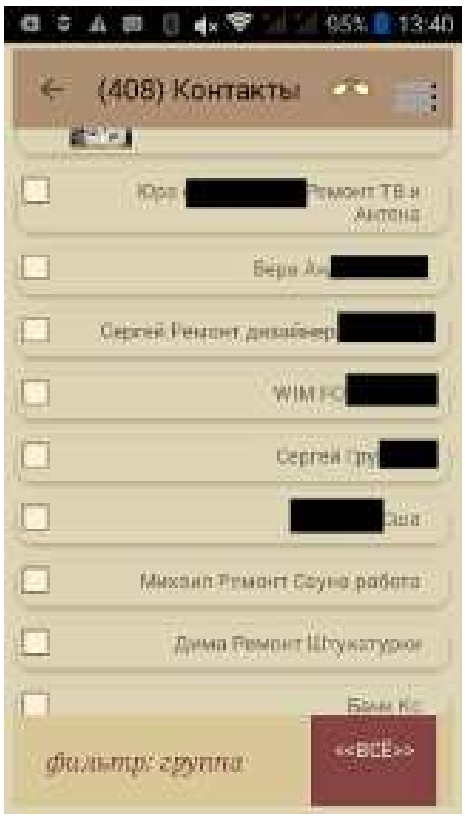


Рис 2.1 Алфавитный список с нешифрованными контактными данными

2.1 АЛФАВИТНЫЙ СПИСОК КОНТАКТОВ

После клика кнопки «Контакты» откроется алфавитный список контактов.

Слева от имени располагается чек-бокс. Отмеченный чек-бокс означает, что у данного контакта имеются зашифрованные данные. Если отметки нет, то поставив её, их можно зашифровать.

Справа от имени может располагаться «Золотой ключ», это означает, что данному контакту приписан персональный крипто-ключ, которым будут шифроваться сообщения, отправляемые на это имя и дешифроваться сообщения от него.

При работе с алфавитным списком можно осуществить следующие действия: 1) шифровать/дешифровать контактные данные выборочно или полностью; 2) сортировать записи алфавитного списка; 3) искать требуемый контакт; 4) открыть «карточку контакта» для выполнения дополнительных действий. 5) сливать дубликатные контакты, если они существуют («профилактика»)

2.1.1 ШИФРОВАТЬ/ ДЕШИФРОВАТЬ ДАННЫЕ

Latebra шифрует данные «Контактов» крипто-ключом Приложения и предотвращает несанкционированный доступ к ним. Шифрование касается также шифрования фотографий. Используя кнопки «Шифровать» (или «Дешифровать») можно зашифровать все контактные данные сразу или выборочно (Рис 2.2).

Мы рекомендуем после того, как все необходимые контакты будут зашифрованы, сохранить результаты. Тогда любой, кто будет смотреть эти данные через стандартное приложение «Контакты», увидит их зашифрованными (Рис 2.3) и не сможет ими воспользоваться.

Рис 2.2 Алфавитный список с шифрованными контактными данными

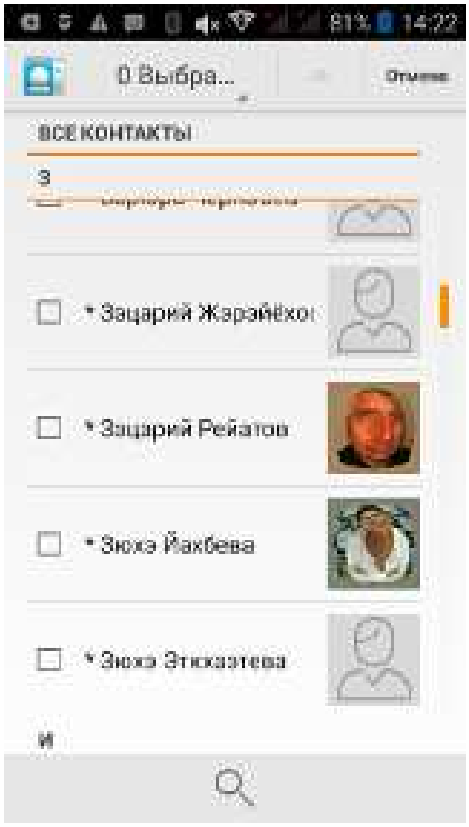


Рис 2.3 Стандартное приложение «Контакты»

Следует также помнить, что если какие-то контактные данные будут дешифрованы и результаты сохранены, то в «Контактах» они также приобретут исходный вид.

2.1.2 СОРТИРОВКА ДАННЫХ

Алфавитный список контактов может быть отсортирован по: 1) именам в алфавитном порядке; 2) фамилиям в алфавитном порядке; 3) времени поступления данных в «Контакты». Процедура сортировки вызывается кликом по кнопке «Сортировка» , которая в свою очередь активизирует контекстное меню, где можно определиться с вариантами сортировки .

2.1.3 ПОИСК

Клик по кнопке «Поиск» вызовет процедуру, помогающую найти требуемый контакт в алфавитном списке. По мере набора букв будет формироваться сужающийся список предлагаемых вариантов. Поиск будет осуществляться одновременно и по фамилии и по имени и по отчеству. Следует особо отметить, что даже если какой-то контакт зашифрован, то это не помешает процедуре поиска.

2.2 КАРТОЧКА КОНТАКТА

Двойной клик по контакту в алфавитном списке открывает «Карточку Контакта» с фотографией контакта и номерами его телефонов и адресами электронной почты. Все эти элементы, включая фотографию, по отдельности или сразу могут быть зашифрованы непосредственно в «Карточке Контакта». Эти элементы «Карточки Контакта» являются контрольными элементами. Клик по имени контакта в карточке покажет его персональный крипто-ключ (если он существует). Клик по номеру телефона вызовет диалог, в котором Вы сможете:

- Отредактировать данные;
- Удалить их;
- Позвонить на выбранный номер телефона;
- Послать SMS\MMS сообщения на данный номер.

Аналогично клик по адресу электронной, вызывает подобный диалог, в котором можно отредактировать или удалить исходные данные или послать Email на выбранный адрес электронной почты.

Если выбран вариант отсылки сообщения, то будет вызван Редактор, где можно будет создать сообщение, зашифровать и отослать его выбранным способом. Шифрование будет осуществляться персональным крипто-ключом данного контакта. Если у данного контакта нет такого ключа, то Вам будет предложено создать и приписать данному контакту крипто-ключ, не выходя из Редактора.

Послать сообщения или позвонить можно даже без предварительной дешифровки контактных данных.

Важно, что «Карточка контакта» предназначена также для генерации персонального ключа, привязки и дистрибуции его данному контакту с возможностью выбора метода отсылки (Email или SMS). Для запуска этой процедуры этого достаточно кликнуть по кнопке «Золотой ключ» .

Рис.2.4 Вид «Карточка контакта» с зашифрованными данными

Помимо вышеизложенного, кликнув кнопку «Переписка» можно посмотреть всю переписку с данным контактом.

2.2.1 ПЕРСОНАЛЬНЫЙ КРИПТО-КЛЮЧ

Клик по кнопке «Золотой Ключ» в «Карточке Контакта», позволит создать (или изменить) и приписать персональный Крипто-ключ данному контакту, а также переслать его, выбрав способ доставки Email или SMS. В дальнейшем он будет использоваться для шифрования/дешифрования сообщений этого адресата. После того как этот персональный ключ будет отослан Вашему корреспонденту и он его сохранит его, шифрование/дешифрование сообщений при общении с ним будет осуществляться в один клик. Latebra при шифровании/дешифровании сообщений, зная адрес корреспондента, сама выберет требуемый крипто ключ.

2.2.2 ПЕРЕПИСКА

Для того чтобы увидеть переписку с конкретным абонентом, нужно кликнуть по кнопке «Переписка» в его «Карточке контакта» и указать какая именно переписка Вас интересует SMS/MMS и/или Email, после этого интересующая Вас переписка будет сформирована. Сообщения будут собраны со всех адресов контакта.

2.2.3 ПРОФИЛАКТИКА

Пользователи часто встречаются с дублированием контактов, что мешает и затрудняет работу с ними. В Latebra предусмотрена специальная операция «Профилактика» , которая позволяет сливать контактные данные из нескольких дублирующих контактов в один.

3 РАБОТА С СООБЩЕНИЯМИ

Для того чтобы начать работать с сообщениями достаточно кликнуть по кнопке «Сообщения» , это обеспечит загрузку сообщений непосредственно в Latebra. Сначала будет вызвано контекстное меню Рис. 3.1, где нужно будет выбрать, с каким типом сообщений планируется работать: SMS/MMS и/или Email. С E-mail сообщениями наиболее эффективно и удобно работать пользователям Gmail и Yandex, т.к. только для них Latebra является E-mail клиентом с функцией шифрования/дешифрования.

Рис 3.1 Фильтр при загрузке сообщений

Рис 3.2 Список сообщений

Пользователям других почтовых сервисов придется работать в режиме copy&paste, т.к. функция загрузки сообщений в Latebra для них недоступна

После того, как выбран тип сообщений и кнопка «Далее» будет загружен список сообщений в соответствие с выбранным фильтром. Клик на сообщении выделит его для следующих действий:

1. загрузить в Редактор вторым кликом для просмотра, дешифрования и подготовки ответного сообщения , которое можно отослать кликом по кнопке ;
2. просмотреть переписку с адресатом данного сообщения, кликнув кнопку Рис. 3.3, при этом отосланные сообщения визуализируются на темном фоне, а принятые на более светлом
3. удалить, кликнув кнопку , как отдельное сообщение, так и всю переписку (только для SMS).

При работе с подключённым E-mail сервисом доступна функция управления аккаунтами, для этого нужно кликнуть кнопку .

Если возникнет необходимость создать и отослать новое сообщение, то нужно только кликнуть кнопку «Новое» и вызвать Редактор, где выполнить все необходимые действия.

Рис 3.3 Переписка

3.1 РЕДАКТОР

Для ускорения и оптимизации работы по подготовке и отсылке новых сообщений предусмотрен прямой вызов Редактора непосредственно из основного окна Приложения кликом по кнопке . Это позволяет подготовить и отослать сообщение без их предварительной загрузки, это важно когда Интернет - «плохой». Вызов Редактора может быть осуществлен также двумя способами:

- Клик по выделенному сообщению для загрузки этого сообщение в Редактор.
- Клик кнопки «Новое» в Редакторе обеспечивает следующую функциональность при работе с сообщениями:

1) создание и редактирование, включая вставку данных из clipboard
2) шифрование/дешифрование
3) сохранение
4) отсылка
5) генерация персональных крипто-ключей.

Если у Вашего корреспондента нет персонального крипто-ключа, он, может быть, создан непосредственно в Редакторе для этого достаточно кликнуть по кнопке «Золотой ключ» .

Рис 3.3 Окно редактора создание сообщения

3.1.1 ШИФРОВАНИЕ СООБЩЕНИЙ

Для обеспечения конфиденциальности переписки необходимо перед отправкой зашифровать подготовленное сообщение, кликнув по кнопке «Шифровать» .

!!! Следует помнить, что у Вашего корреспондента на мобильном устройстве также должен быть Latebra.

Шифрование осуществляется персональным крипто-ключом. Если у Вашего адресата его еще нет, персонального крипто-ключа, его нужно предварительно создать и распространить, использую «Карточку Контакта», или его можно создать непосредственно в Редакторе кликнув по кнопке «Золотой ключ» . После генерации персонального крипто-ключа, его нужно отправить вместе с сообщением, тем самым приглашая данного корреспондента войти в Ваш круг доверия. Когда Ваш корреспондент сохранит у себя этот крипто-ключ, он тем самым войдет в «экосистему Latebra» и сможет конфиденциально переписываться с Вами, не задумываясь о том, каким крипто-ключом осуществляется шифрование/дешифрование.

Рис 3.3 Окно редактора с шифрованным сообщением

Если инициатором конфиденциальной переписки выступает Ваш корреспондент, то он должен отправить Вам сообщение с персональным крипто-ключом. При открытии этого сообщения Вам

будет предложено приписать данный крипто-ключ к его адресным данным, естественно, этот корреспондент должен быть у Вас в «Контактах».

3.1.2 ДЕШИФРОВКА СООБЩЕНИЙ

Если получено шифрованное сообщение, то оно дешифруется кликом по кнопке «Дешифровать» в Редакторе. Дешифровка будет осуществлена в один клик, если корреспонденту был приписан Персональный крипто-ключ. Следует иметь в виду, что эта возможность наиболее удобно реализуется для SMS/MMS сообщений или, если идет речь об Email, только для сервисов Gmail или Yandex, для которых Latebra становится Email клиентом с функцией шифрование/дешифрование.

Сообщение также может быть дешифровано крипто-ключом, присланным вместе с сообщением. Получив крипто-ключ вместе с сообщением, Вам будет предложено привязать его к контактным данным Вашего корреспондента как персональный крипто-ключ или использовать присланный ключ для дешифровки только данного сообщения.

После прочитывания сообщения его можно удалить, для этого достаточно кликнуть .

Рис 3.4 Окно редактора с дешифрованным сообщением

Мы рекомендуем, после получения сообщения с крипто-ключом и приписывания его, удалить это сообщение!!!

3.1.3 КРИПТО-КЛЮЧ

Кликнув кнопку «Золотой ключ» в Редакторе можно сгенерировать Персональный Крипто-Ключ. Приписать Персональный Крипто-Ключ можно только адресату, который есть в Ваших «Контактах».

3.1.4 СОХРАНИТЬ ЧЕРНОВИК

Подготовленное сообщение с адресом из адресной строки Редактора (или с пустой адресной строкой) можно сохранить, как черновик . Следует помнить, что при сохранении черновика предыдущий черновик с данным адресом будет заменен этим. Новый черновик без адреса также заменяет старый без адреса.

3.1.5 ОТКРЫТЬ ЧЕРНОВИК

Клик на кнопке «Открыть» откроет черновик с адресом, который в данный момент находится в адресной строке Редактора. Если адресная строка пустая, то откроется последний сохраненный черновик без адреса или новое сообщение, если безадресных черновиков нет.

3.1.6 ПОСЛАТЬ СООБЩЕНИЕ

Сообщение будет послано по адресу, указанному в адресной строке, если кликнуть по кнопке «послать сообщение» . Отсылаемое сообщение может быть как зашифрованным, так и нет. При отсылке зашифрованного сообщения будет предложено дополнить сообщение персональным крипто-ключом.

МЫ РЕКОМЕНДУЕМ ОТСЫЛАТЬ КРИПТО-КЛЮЧ ТОЛЬКО В ПЕРВЫЙ РАЗ.

3.1.7 АДРЕСНАЯ СТРОКА

При вводе адреса в Адресной Строке работает подсказка, использующая данные «Контактов». Если адресат отсутствует в «Контактах», его адрес придется набирать вручную. Допускается поиск, как по имени адресата, так и непосредственно по адресу или телефону.

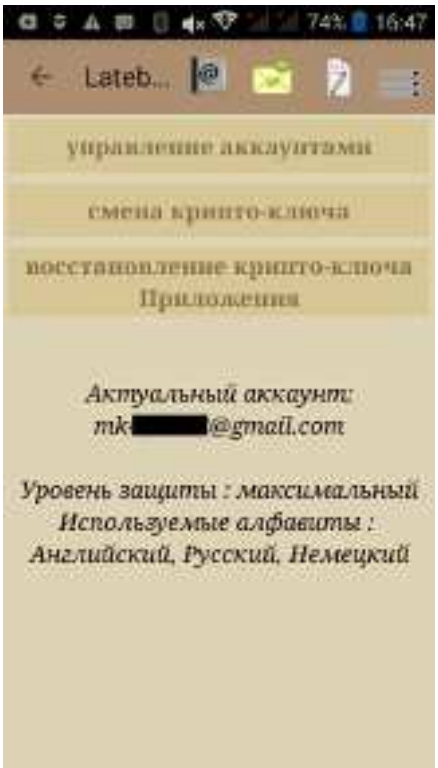
Если у владельца введенного адреса имеется персональный крипто-ключ, то «Золотой ключ" будет виден в Адресной Строке. В режиме ответа в Адресную Строку будет автоматически помещён адрес, на который следует отсылать сообщение.

3.1.8 РАБОТА С СООБЩЕНИЯМИ В РЕЖИМЕ COPY&PASTE

Пользователям отличных от Gmail и Yandex сервисов придется пользоваться режимом copy&paste. В этом случае Latebra уже не будет E-mail клиентом, а будет только редактором с функцией шифрования/дешифрования. В частности, у подобных пользователей не будет возможности шифровать/дешифровать E-mail в один клик.

При получении шифрованного сообщения в соответствующем E-mail клиенте нужно будет его полностью скопировать и вставить в Редактор Latebra , где, используя присланный крипто-ключ, расшифровать. Если ключ не был прислан, то придется в адресной строке Редактора набрать адрес отправителя данного сообщения или скопировать его из сообщения и после этого расшифровать, используя персональный крипто-ключ данного адресата.

Рис 3.5 Стандартное E-mail приложения



4 НАСТРОЙКА

Вы всегда можете изменить параметры Latebra выбранные изначально, используя кнопку «Настройка» В режиме "Настройка" Вы можете:

1) проверить уже введенные данные или подключить новые почтовые аккаунты (только Gmail и Yandex); 2) сгенерировать новый крипто-ключ Приложения; 3) восстановить крипто-ключ Приложения.

Следует помнить, что после смены крипто-ключа Приложения ВСЁ ранее зашифрованное этим ключом нельзя будет дешифровать новым крипто-ключом Приложения. Настоятельно рекомендуется перед сменой крипто-ключа Приложения дешифровать ВСЁ ранее им зашифрованное. Если же Вы, все-таки, забудете дешифровать ВСЁ ранее им зашифрованное, то Вы сможете временно восстановить предыдущие крипто-ключи Приложения, зная кодовые слова, используемые при их генерации, и приблизительное время, когда они были созданы.

Рис 3. Настройки