

# Памятка о том, как защитить себя и своих близких при использовании сети Интернет

**Евгений Солянкин**

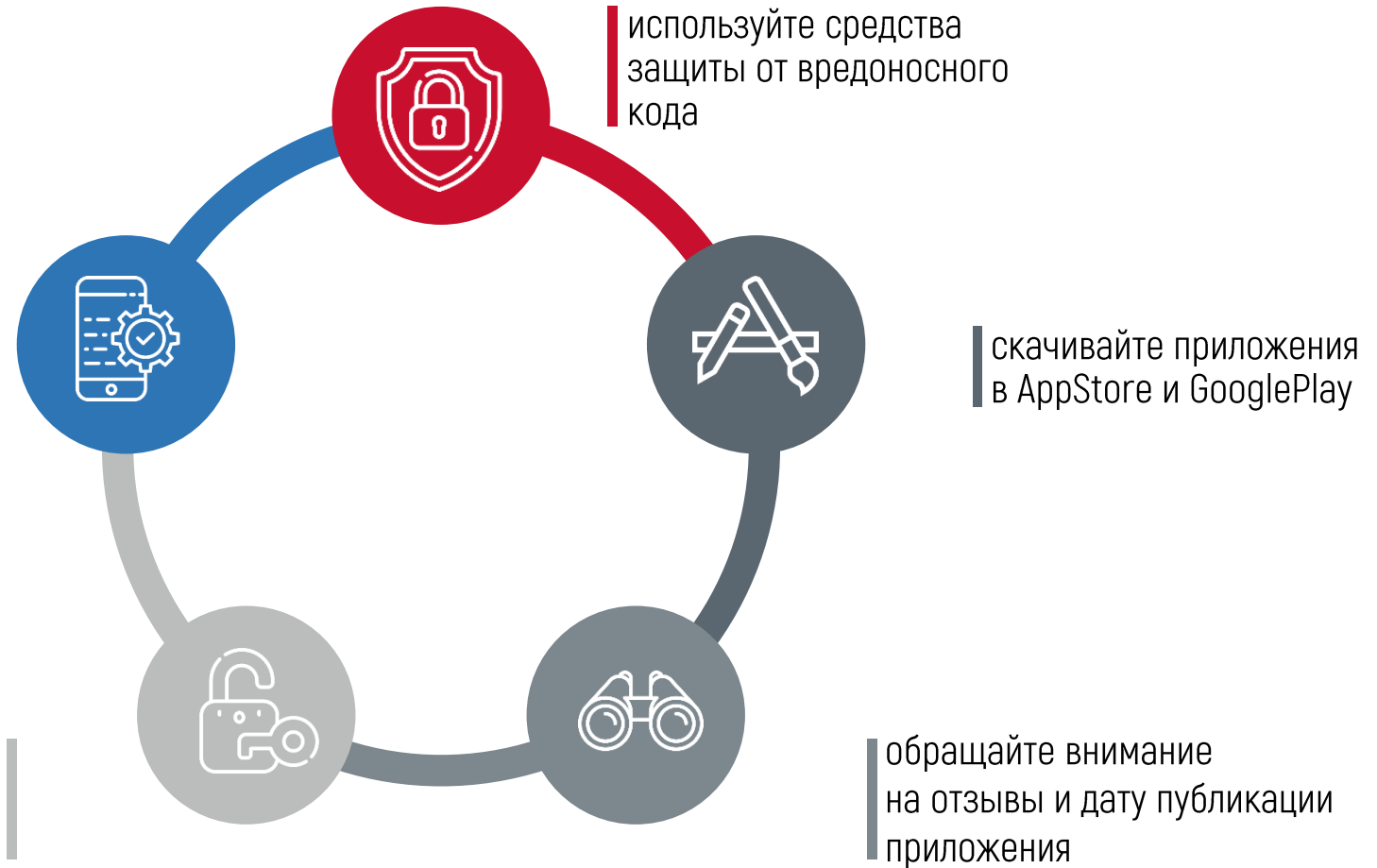
Руководитель Управления информационной безопасности



# Как защитить свой смартфон



# Все, что нужно знать о защите своего телефона



# Как не стать жертвой фишинга



# Как распознать фишинг



## неизвестный отправитель

- ✓ вы не знаете отправителя
- ✓ почтовый адрес похож на корпоративный, но есть отличия



## побуждение к действию

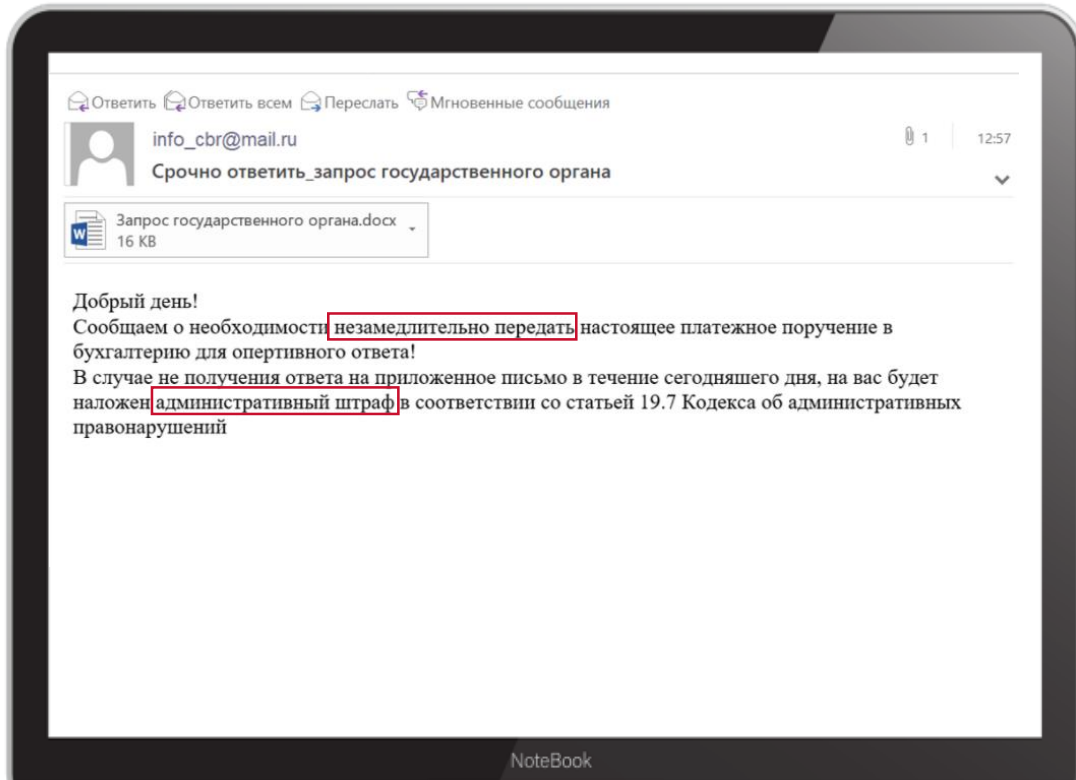
- ✓ «срочно подпишите» или «передайте»
- ✓ угрозы штрафом
- ✓ воздействие на Ваше любопытство или обещание бесплатных благ



## странные вложения

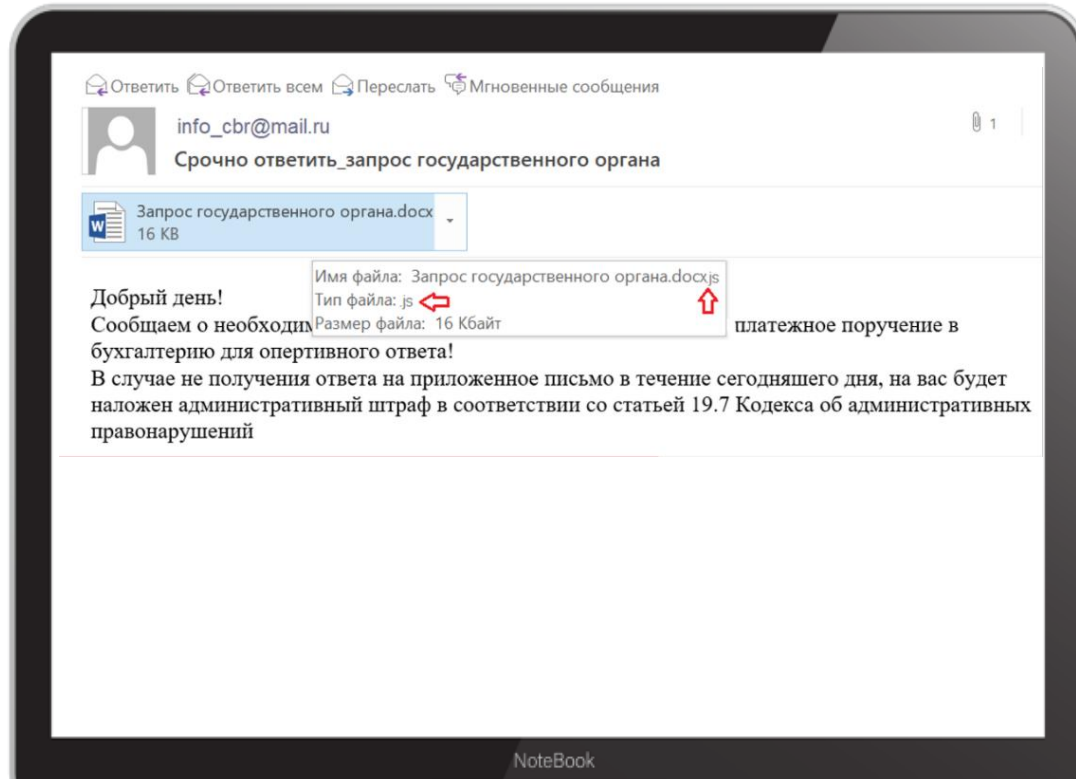
- ✓ вложения формата .EXE, .BAT, .DAT, JS, то есть не являющиеся MS Office или картинками

# Как выглядят реальные инциденты



- ✗ сообщение отправлено с общедоступного ящика @mail.ru. Это не похоже на официальный запрос регулятора
- ✗ нет контактных данных отправителя
- ✗ призыв к незамедлительному действию (передать документ в бухгалтерию)
- ✗ угроза наложения денежного штрафа

# Как выглядят реальные инциденты



на самом деле приложенный файл является исполняемым файлом в формате .js. Письмо содержит вредоносное вложение



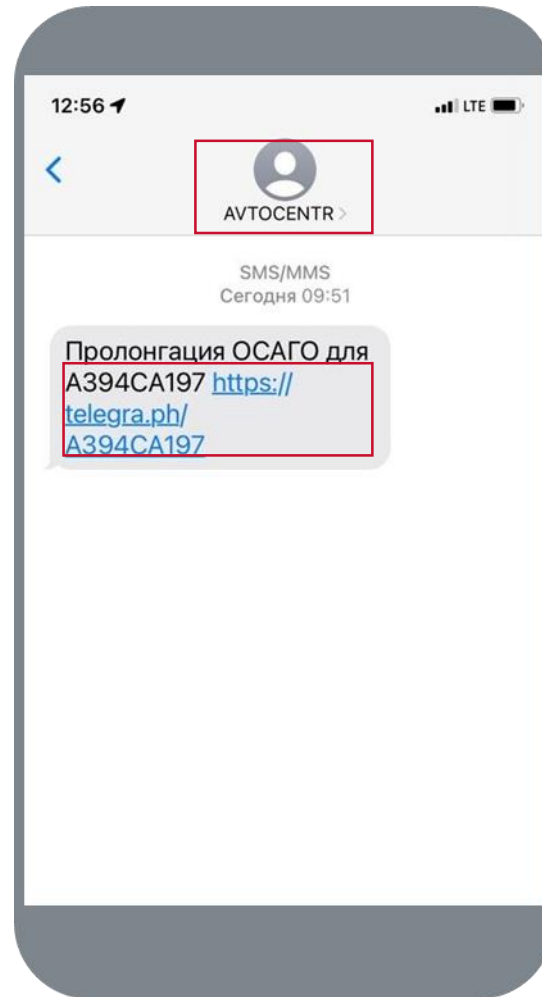
таким образом, совершенно понятно, что Вы столкнулись с фишингом



# Как это бывает, когда фишинг ориентирован на клиента

клиенту поступил звонок от робота  
о необходимости оплатить договор

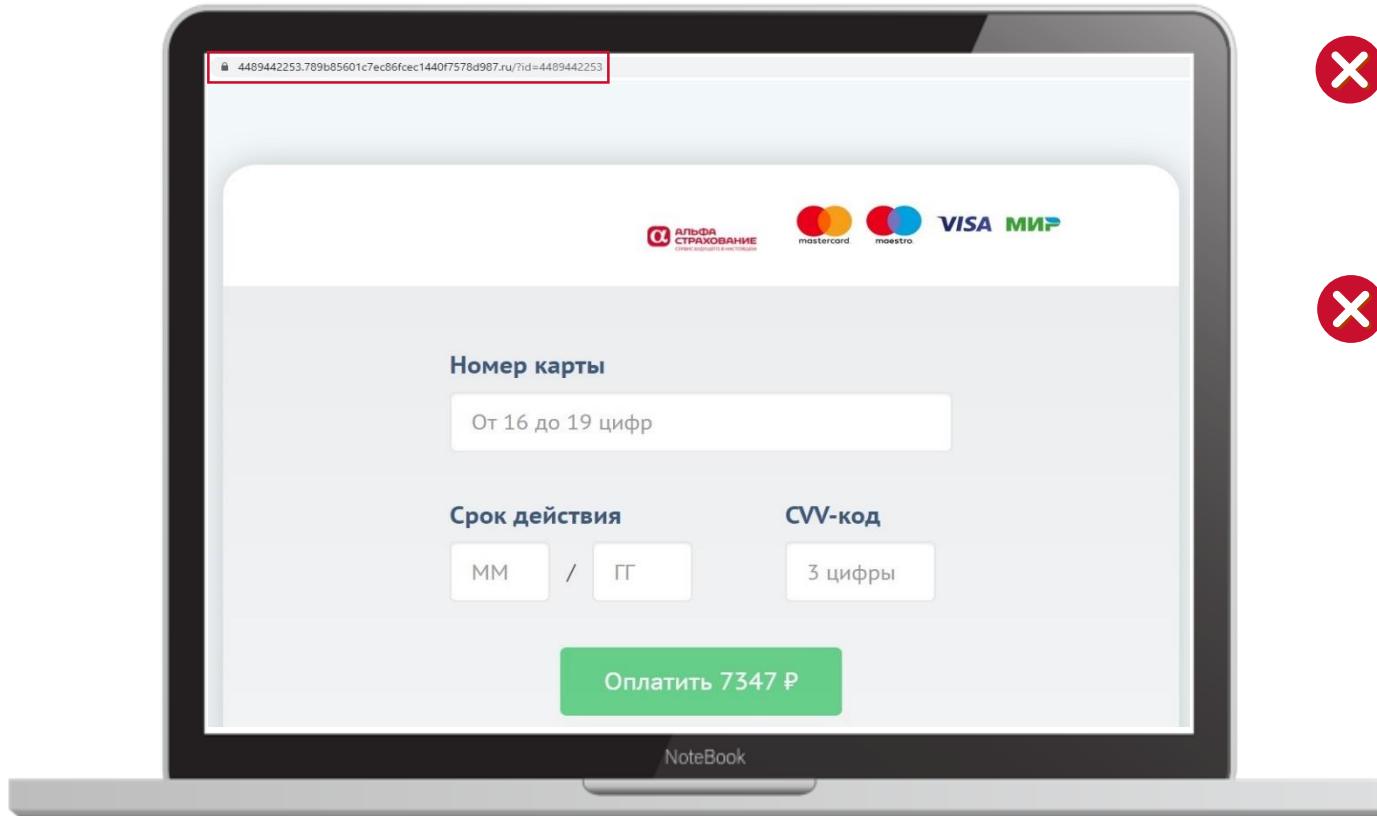
на телефон клиента была  
направлена ссылка на оплату



- ? обращайтесь внимание на отправителя. Если он не известен Вам, то переходить по ссылке – плохая идея
- ? ссылка из сообщения относится к открытой блог-платформе Telegraph, на ее основе очень просто создать любую страницу-переходник
- ? страховая никогда не указывает атрибуты объекта страхования



# Как это бывает, когда фишинг ориентирован на клиента



адрес страницы не содержит идентификаторов платежного оператора. Вместо них лишь произвольный набор символов



логотип АО «АльфаСтрахование» стоит в одном ряду с платежными системами, что странно, т.к. страховая компания не имеет отношения к выполнению переводов денежных средств



таким образом совершенно понятно, что Вы столкнулись с фишингом

# Что делать, если Вы обнаружили фишинг:

1



не переходите  
по ссылкам  
из письма

2



не открывайте  
и не скачивайте вложенные  
файлы

3



удалите  
фишинговое  
письмо

4



расскажите  
о случившемся  
службе ИБ

# Как защититься от телефонных мошенников



# Первый лайфхак, чтобы перестать бояться телефонных МОШЕННИКОВ



вас беспокоят  
«из службы безопасности банка»



вас просят предоставить  
свои персональные данные  
«для проверки» чего-нибудь



вас просят сообщить реквизиты банковских  
карт: номер, срок действия, владелец, CVV



«скажите мне код подтверждения, который  
придет по СМС»



просто положите трубку и  
перезвоните в банк  
самостоятельно

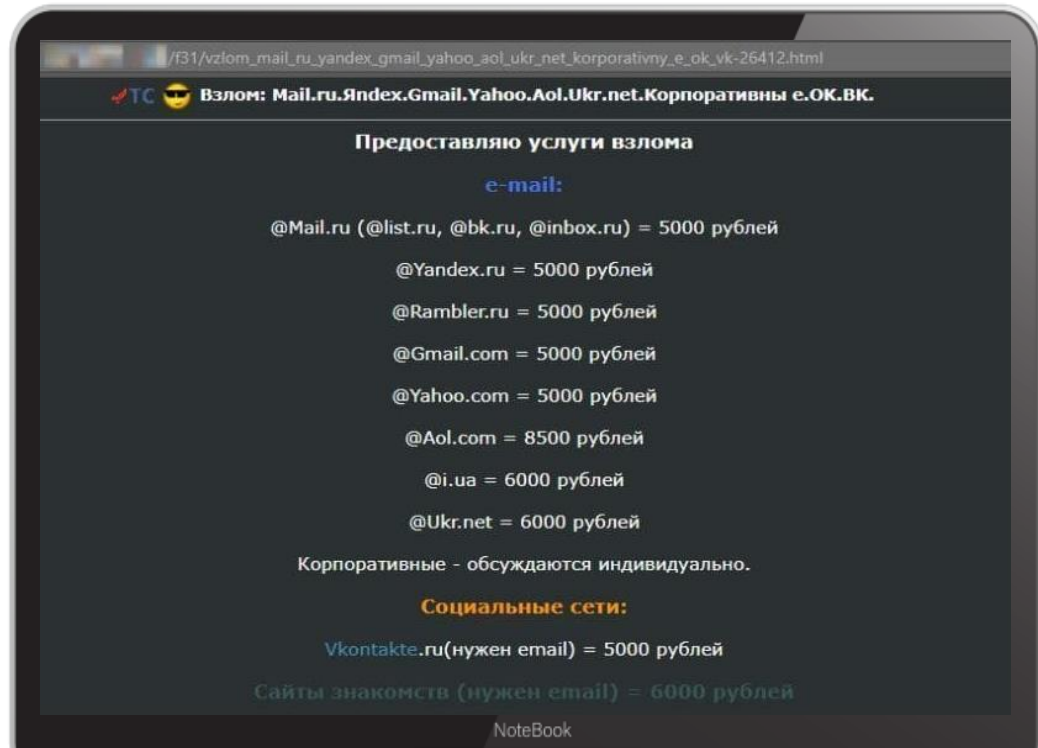
Второй лайфхак, чтобы перестать бояться телефонных мошенников – установите определитель номера



# Как защитить свой электронный почтовый ящик



# Будьте уверены в защите своего почтового ящика



Придумайте сложный пароль, чем пароль длиннее, тем сложнее его взломать. Использование разных регистров и добавление символов не панацея



используйте двухфакторную аутентификацию



обновляйте приложения до последней версии



отправляйте конфиденциальную информацию в архивах с паролем. Передавайте пароль получателю через иной канал



не сохраняйте пароли в браузере и очищайте кэш браузера, историю посещённых сайтов, cookies



пользуйтесь программными хранилками паролей (KeePass, Trezor Password Manager или любым другим по вкусу)

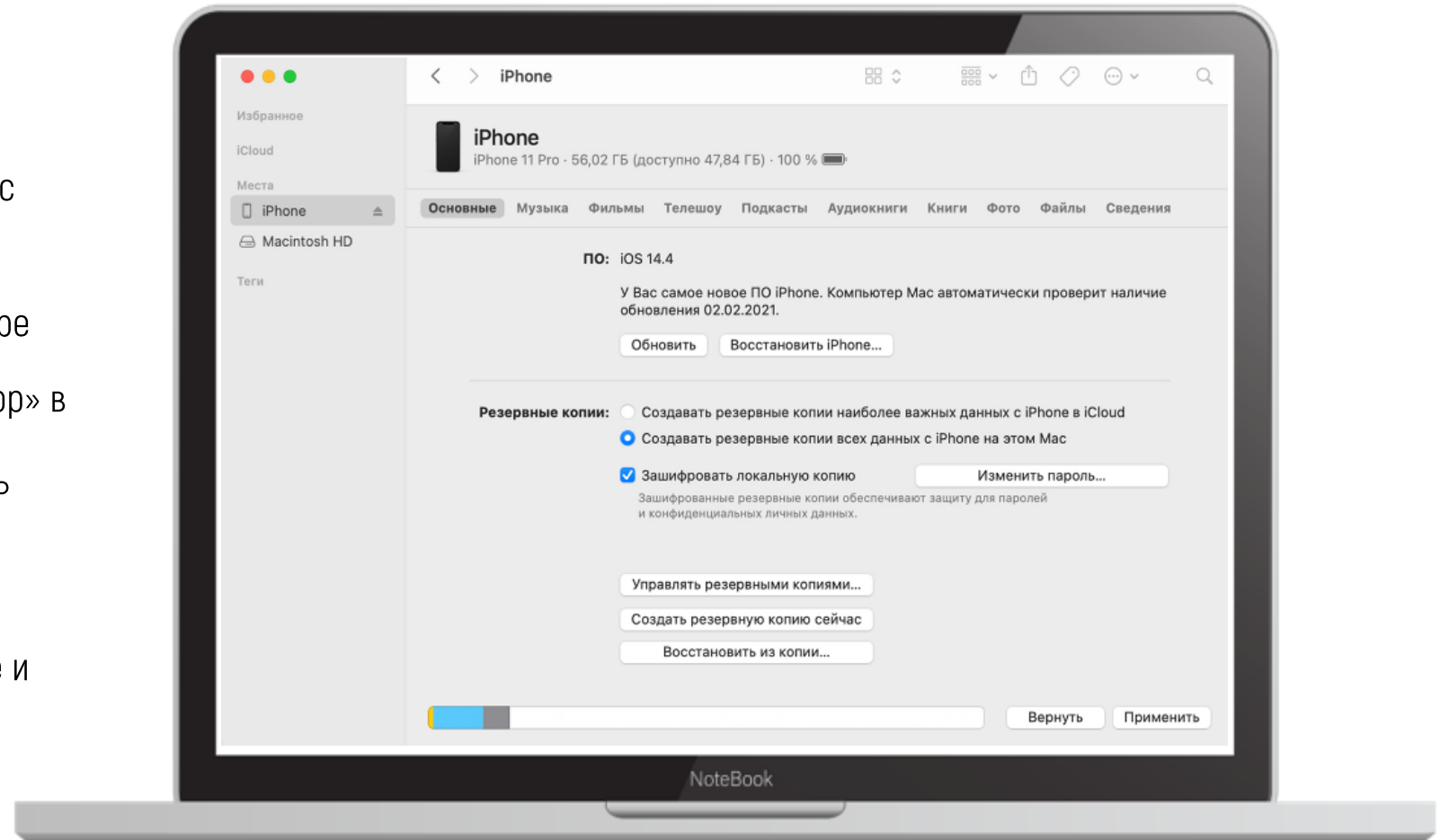


# Как зашифровать резервные копии смартфонов

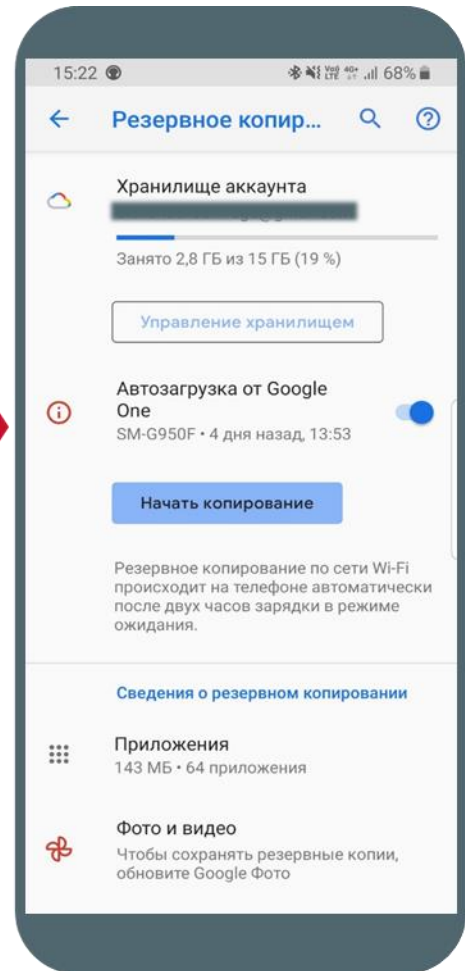
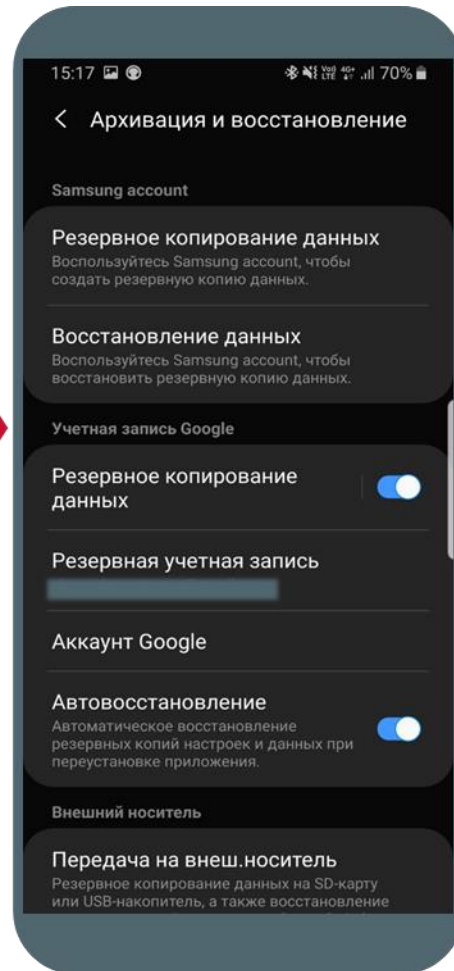
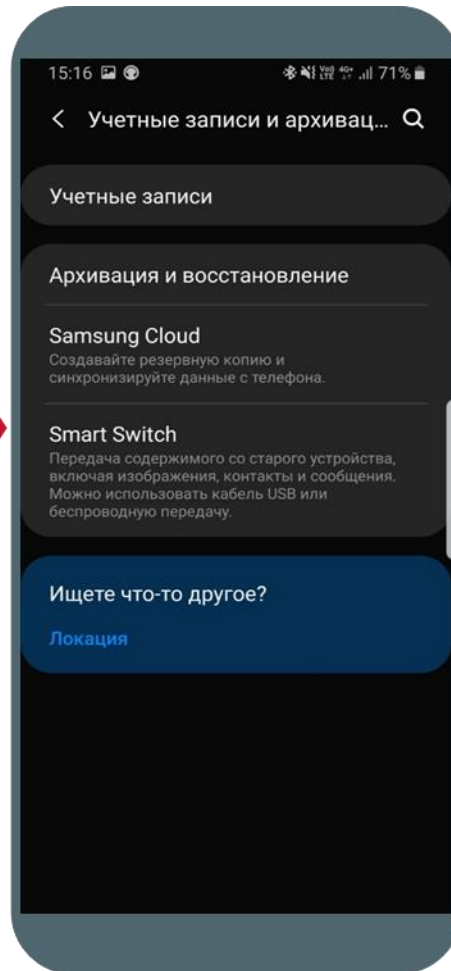
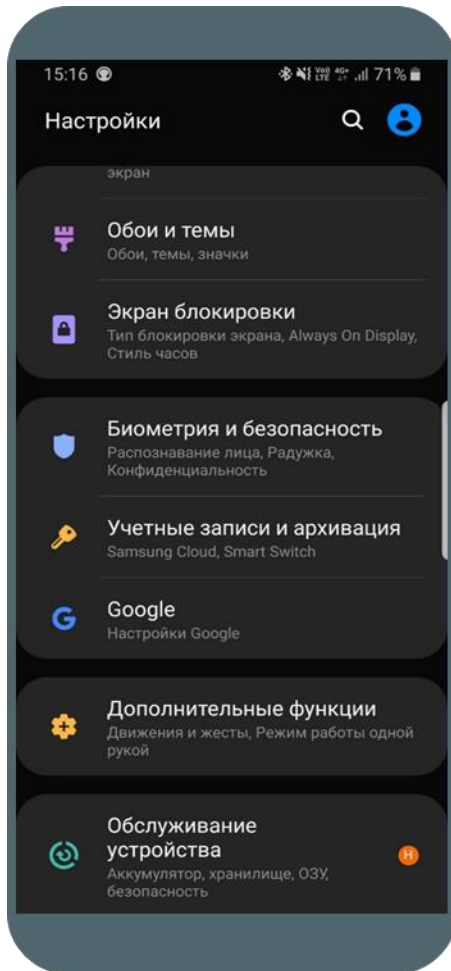


# Создание зашифрованной резервной копии iPhone

- ✓ Включите приложение iTunes на компьютере
- ✓ Подключите iPhone к компьютеру с помощью кабеля Lightning
- ✓ Найдите свой iPhone на компьютере
- ✓ На вкладке «Основные» или «Обзор» в разделе «Резервные копии» установите флажок «Зашифровать локальную копию»
- ✓ Когда появится соответствующий запрос, создайте пароль, который сможете запомнить, или запишите и сохраните его в надежном месте



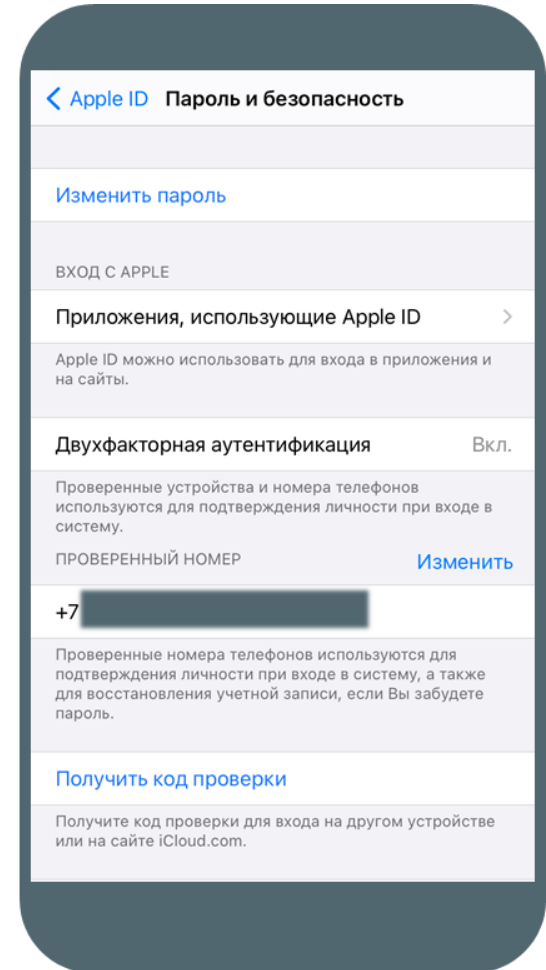
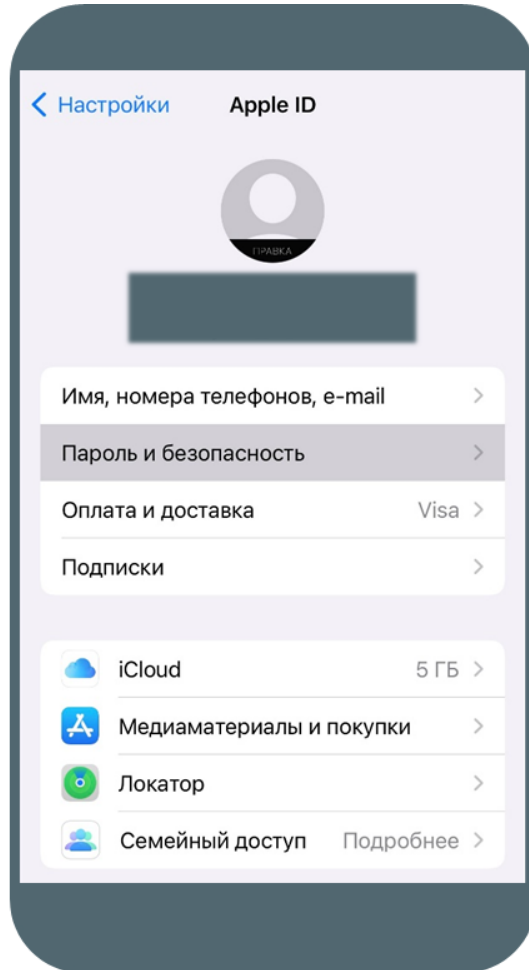
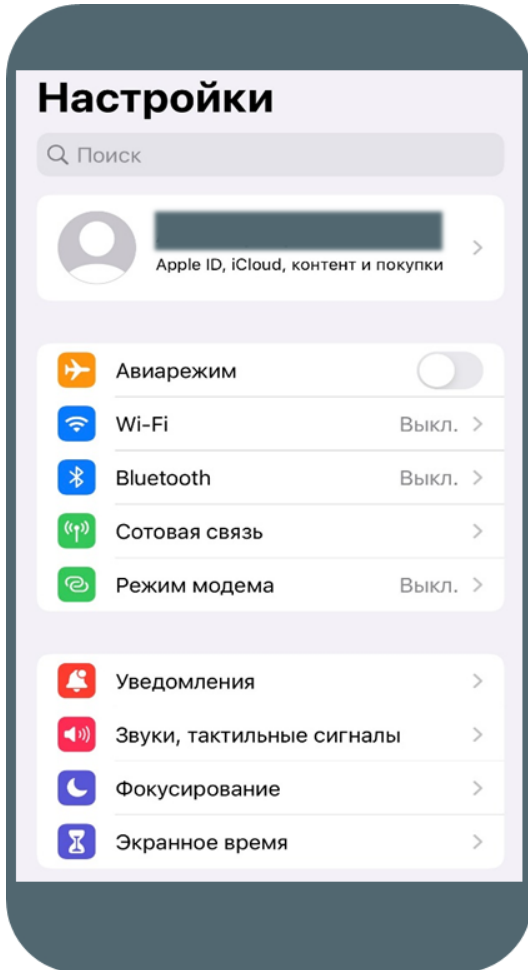
# Создание резервной копии Android



# Как настроить двухфакторную аутентификацию

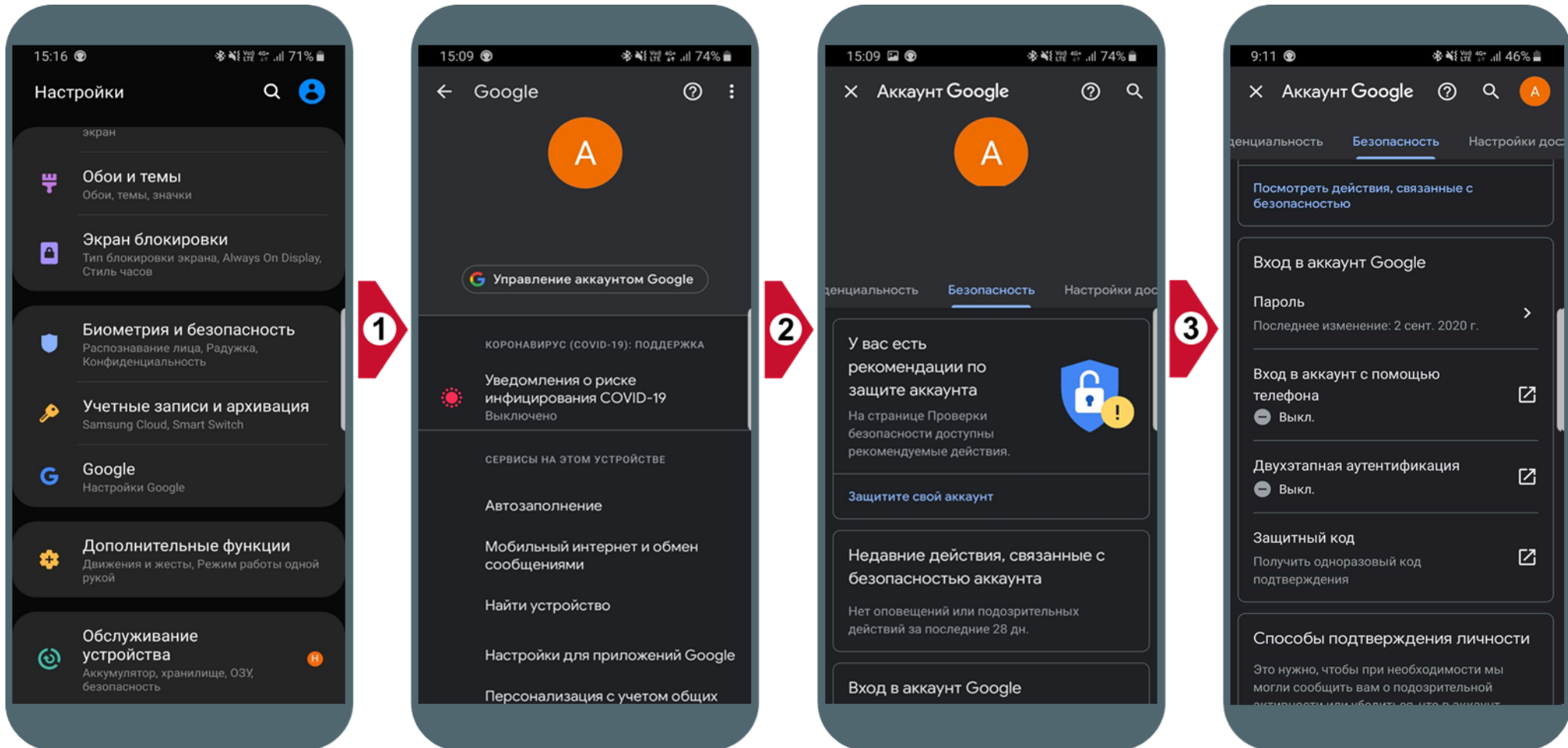


# Двухфакторная авторизация в iPhone





# Двухфакторная авторизация в Android

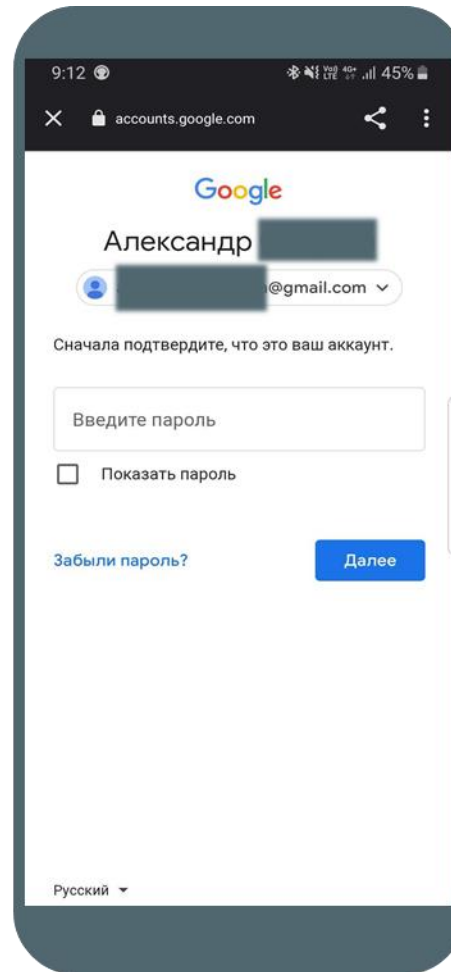


# Двухфакторная авторизация в Android

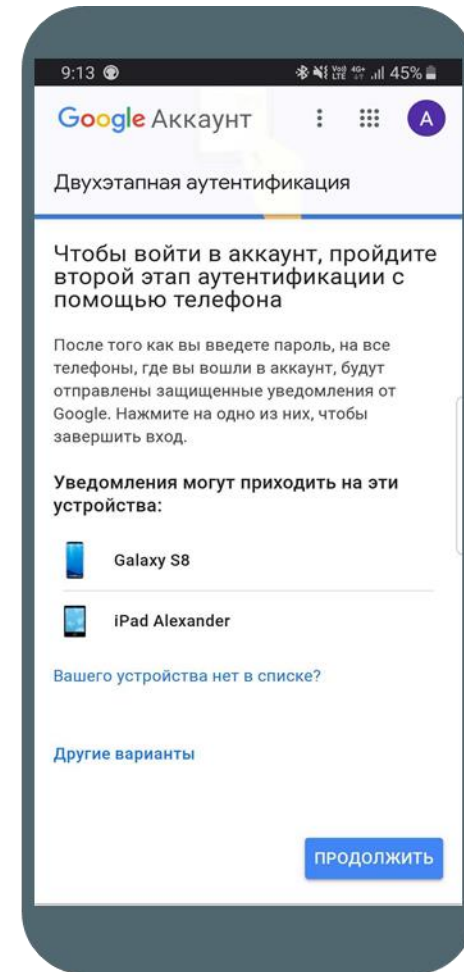
4



5



6





# Двухфакторная авторизация в Android

7

9:13

Google Аккаунт

Двухэтапная аутентификация

Почти готово! Добавьте резервный способ входа.

С помощью резервного способа вы сможете войти в аккаунт, даже если второй этап аутентификации станет недоступен (например, если вы потеряете телефон).

+7 9 [redacted]

Google будет использовать это номер исключительно для защиты аккаунта.  
Не указывайте номер Google Voice.  
Мобильный оператор может взимать плату за передачу данных.

Как вы хотите получать коды?

SMS  Телефонный звонок

ИСПОЛЬЗОВАТЬ ДРУГОЙ СПОСОБ **ОТПРАВИТЬ**

Конфиденциальность Условия

8

9:14

myaccount.google.com

Google Аккаунт

Двухэтапная аутентификац...

Подтверждение номера

Сообщение с [redacted] отправлено на номер 8 (9 [redacted]).  
Введите код

Ничего не получили? Повторить попытку

НАЗАД **ДАЛЕЕ**

Конфиденциальность Условия

9

9:14

Google Аккаунт

Двухэтапная аутентификация

Включить двухэтапную аутентификацию?

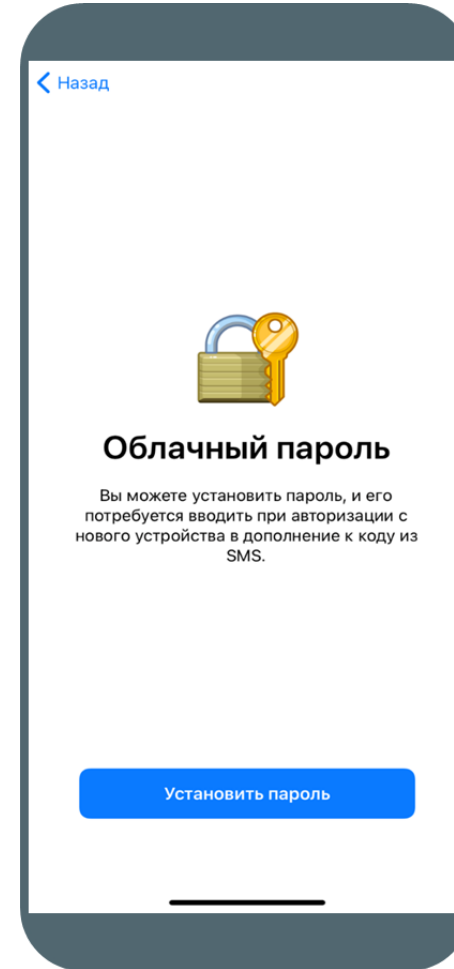
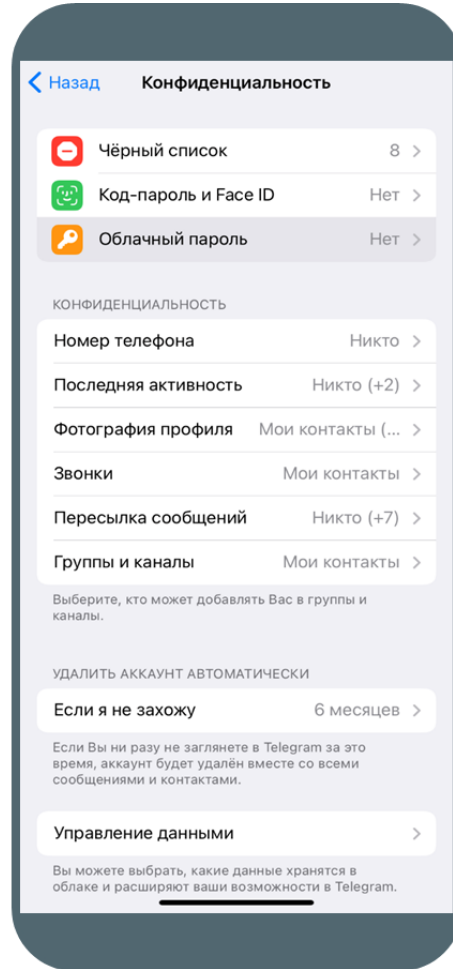
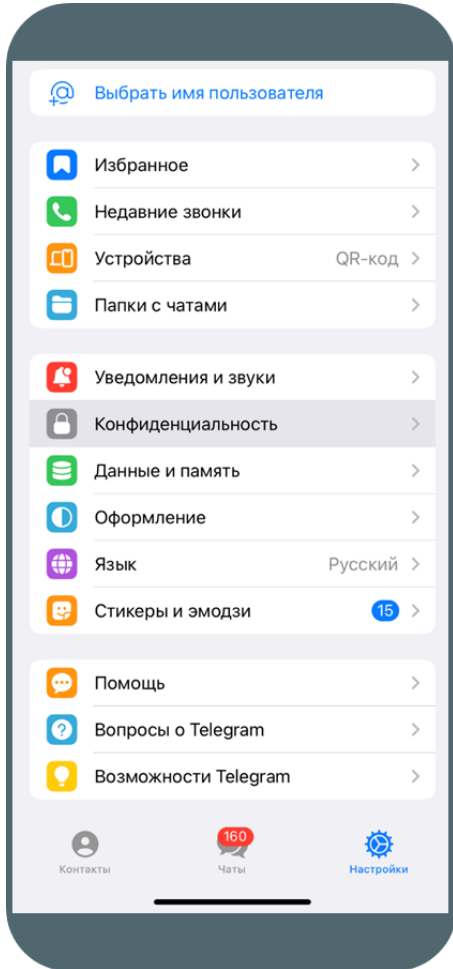
Второй этап: Уведомление от Google (по умолчанию)  
Резервный метод: Голосовое сообщение или SMS

Доступ к аккаунту [redacted]@gmail.com сохранится на этих устройствах: Galaxy S8 и iPad Alexander.

Возможно, на других устройствах вы выйдете из аккаунта. Чтобы снова выполнить вход, нужно будет ввести пароль и пройти второй этап аутентификации.

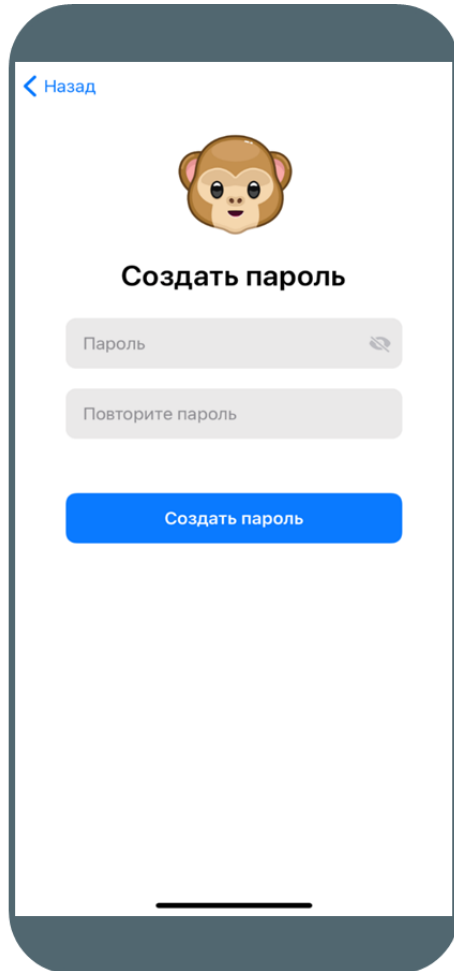
**ВКЛЮЧИТЬ**

# Двухфакторная авторизация в Telegram




# Двухфакторная авторизация в Telegram

3



Назад



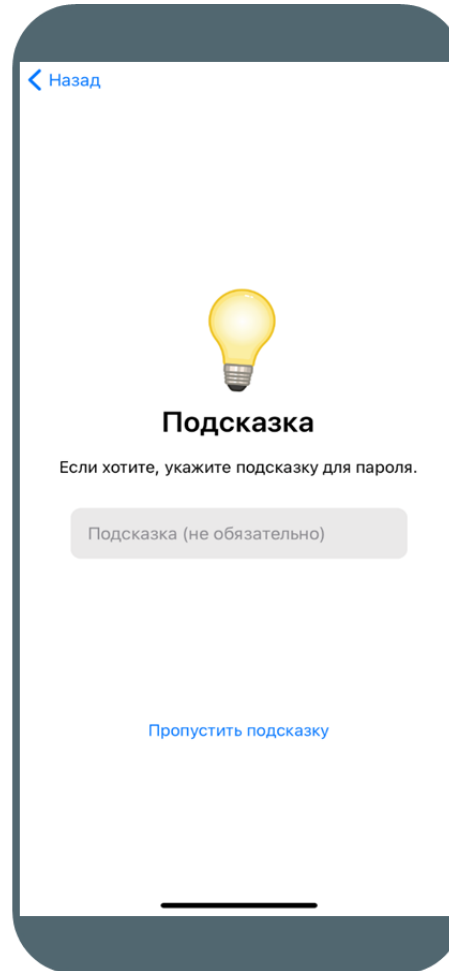
**Создать пароль**

Пароль


Повторите пароль

Создать пароль

4



Назад



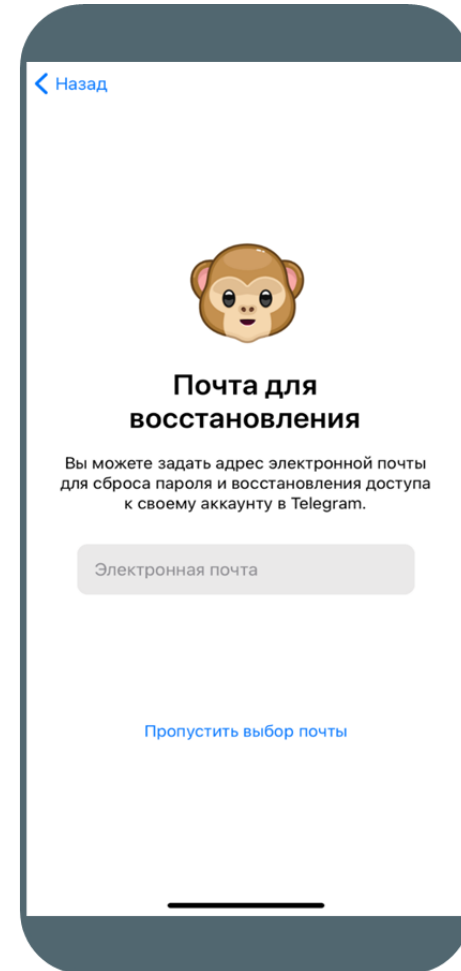
**Подсказка**

Если хотите, укажите подсказку для пароля.


Подсказка (не обязательно)

Пропустить подсказку

5



Назад



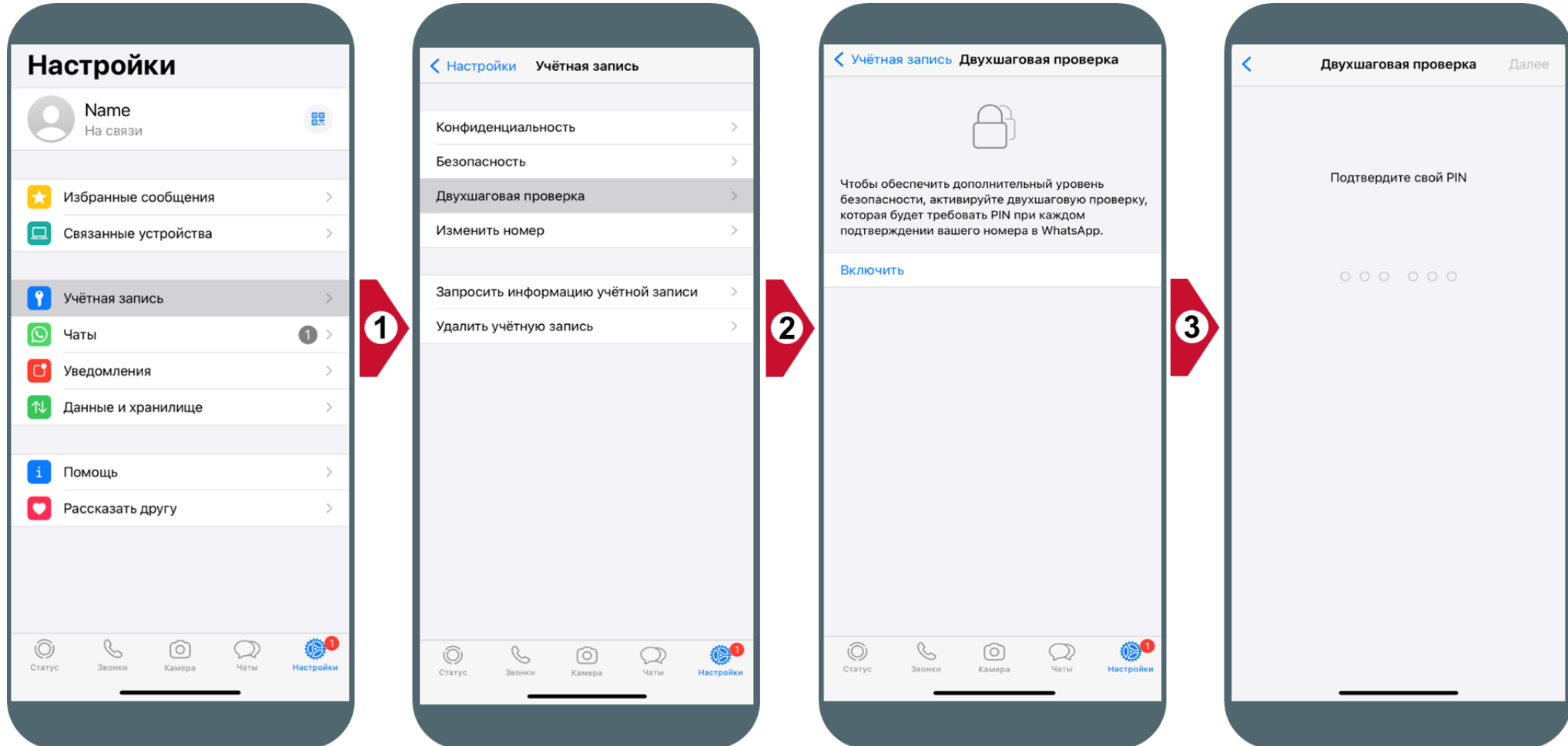
**Почта для  
восстановления**

Вы можете задать адрес электронной почты для сброса пароля и восстановления доступа к своему аккаунту в Telegram.

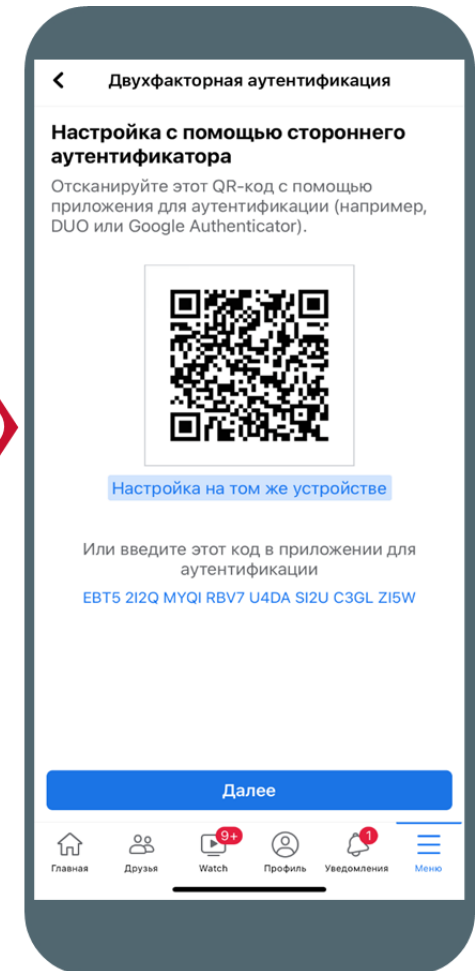
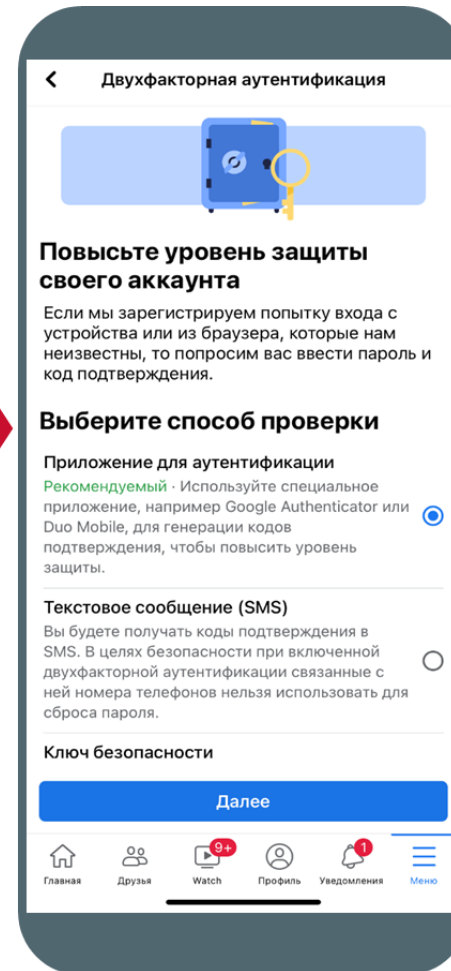
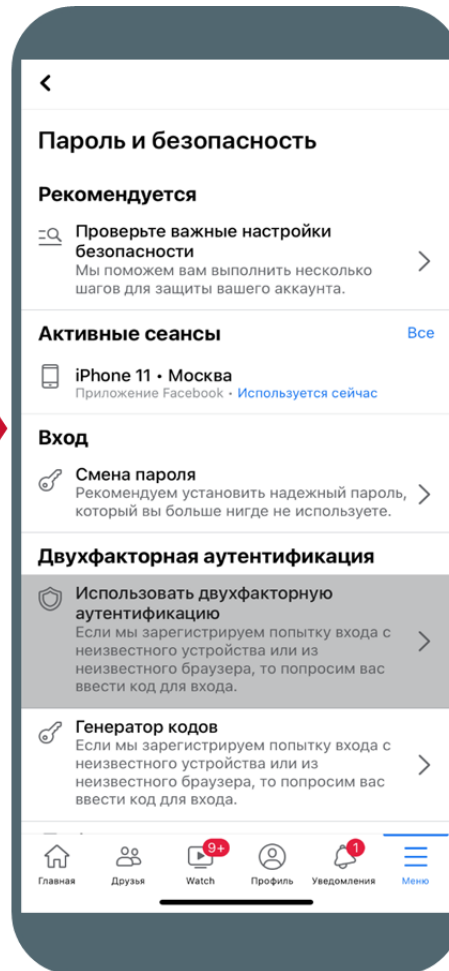
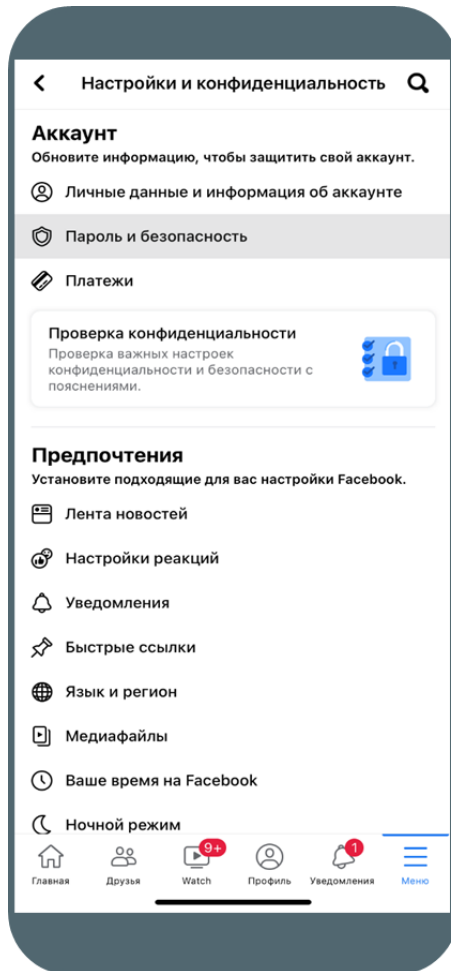
Электронная почта

Пропустить выбор почты

# Двухфакторная авторизация в WhatsApp



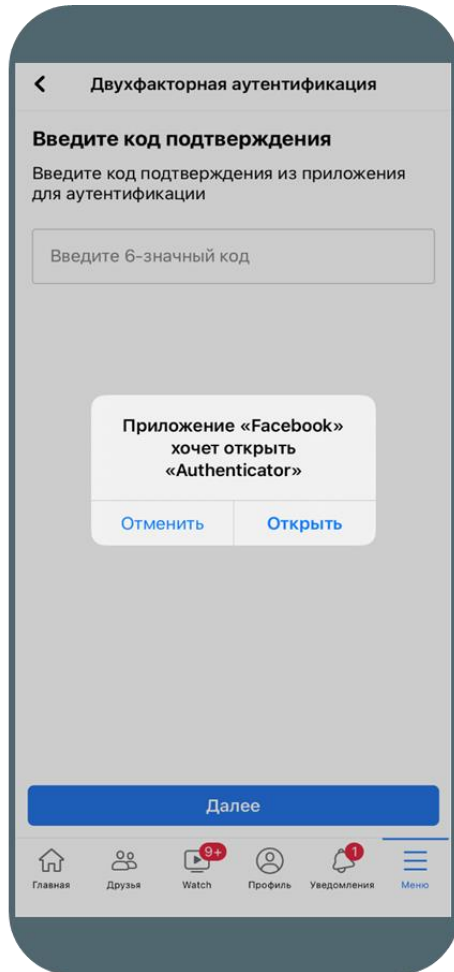
# Двухфакторная авторизация в Facebook\*



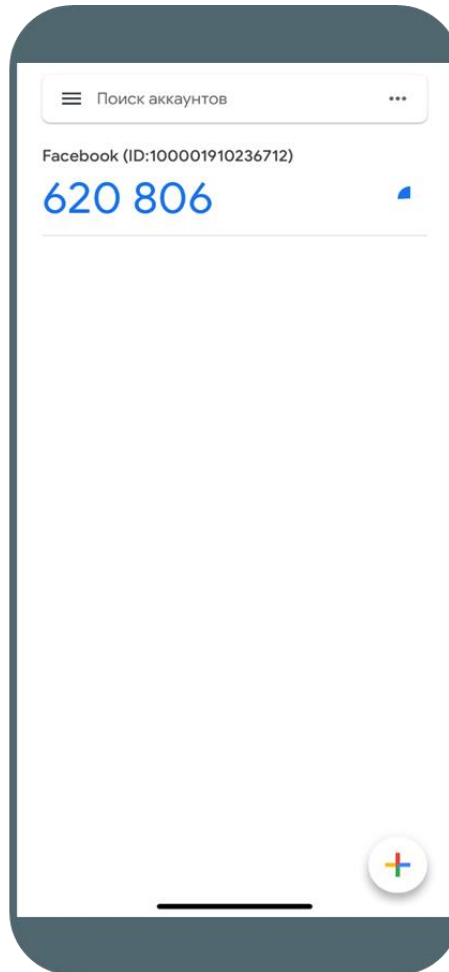
\* Является экстремистской организацией

# Двухфакторная авторизация в Facebook\*

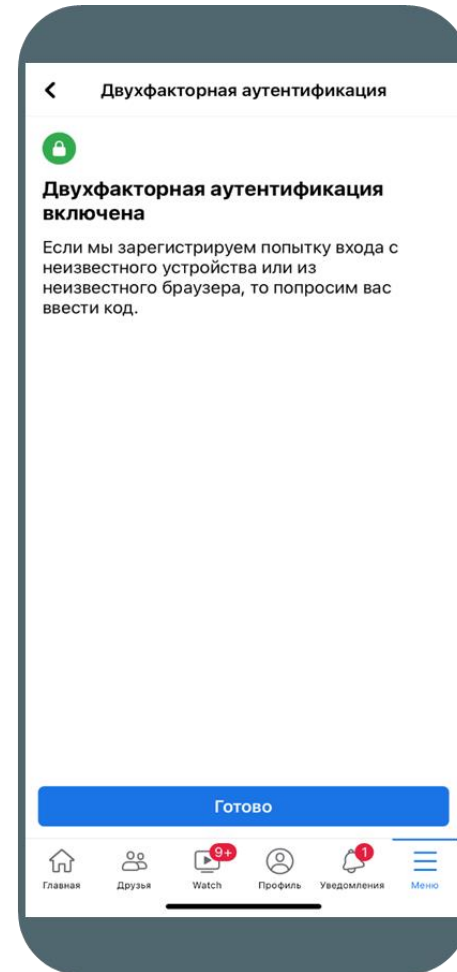
4



5

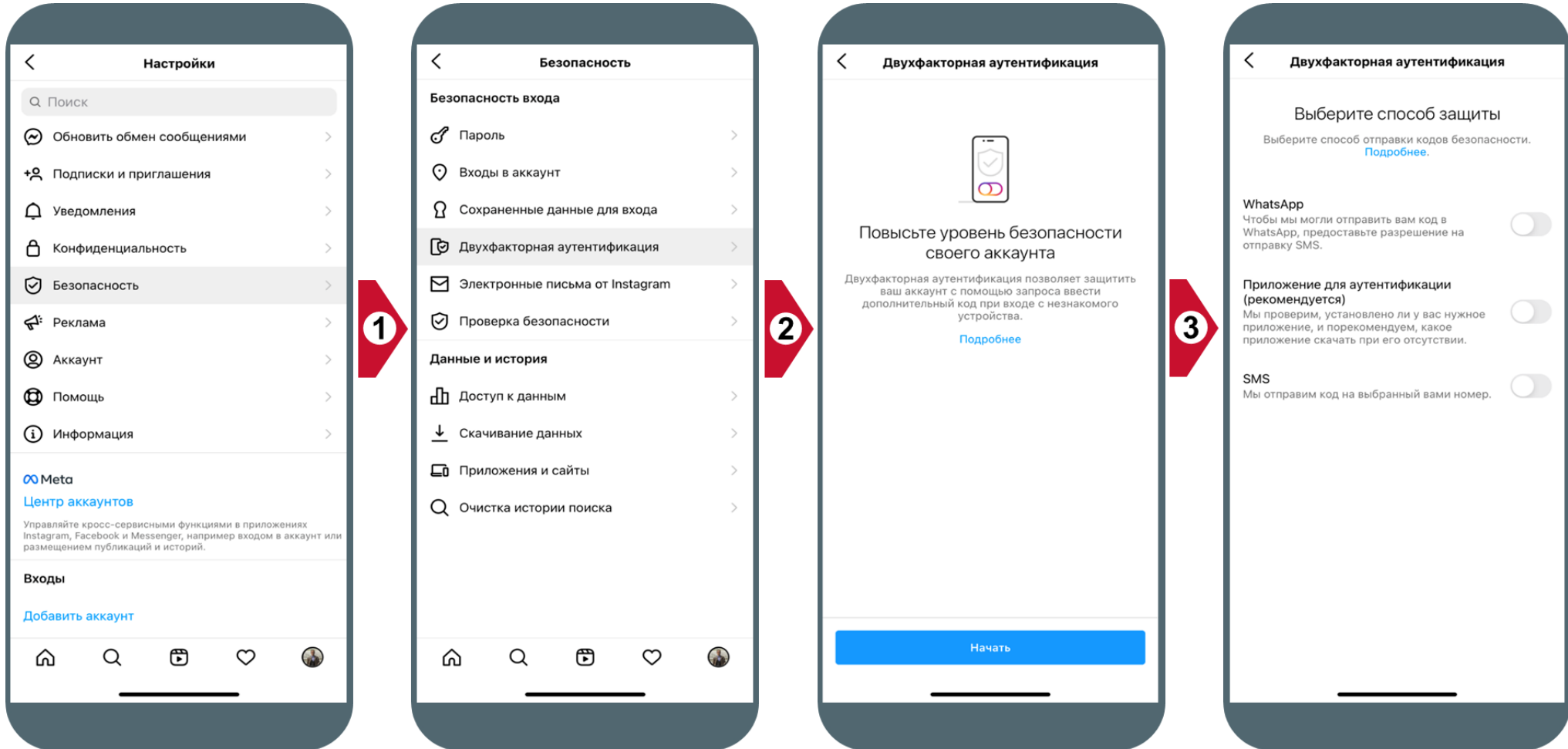


6



\* Является экстремистской организацией

# Двухфакторная авторизация в Instagram\*



\* Является экстремистской организацией



# Двухфакторная авторизация в Instagram\*



**Код подтверждения**

Введите код

Для завершения настройки двухфакторной аутентификации введите 6-значный код, отправленный нами на ваш номер, заканчивающийся на 6699.

0 1 2 3 4 5

**Далее**

Отправить код повторно · Изменить номер телефона

1	2 А Б В Г	3 Д Е Ж З
4 И Й К Л	5 М Н О П	6 Р С Т У
7 Ф Х Ц Ч	8 Ш Щ Ъ Ы	9 Ь Э Ю Я
0		



**Резервный код**

Резервные коды

Если вы потеряете телефон или не сможете получить код с помощью текстового сообщения или приложения для аутентификации, то восстановить доступ к аккаунту можно будет с помощью этих кодов. Сохраните их в надежном месте.

**3675 2014**  
**2893 5416**  
**6453 8017**  
**6249 0857**  
**5678 3094**

Каждый код можно использовать только один раз. Если вы опасаетесь, что этот набор кодов могли украсть, или большая часть кодов уже использована, вы можете получить новые коды.

[Снимок экрана](#) · [Получить новые коды](#)

**Далее**



**Подтверждение**

Двухфакторная аутентификация включена

Мы будем отправлять SMS с кодом на этот номер при каждой попытке входа с неизвестного устройства.

[Подробнее](#)

Получать коды для входа через WhatsApp

Получайте коды безопасности быстрее и надежнее с помощью WhatsApp

**Далее**

\* Является экстремистской организацией