МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования
«Академия Министерства внутренних дел Республики Беларусь»

ПАМЯТКА

«По установке двухфакторной аунтефикации на наиболее популярные приложения и мессенджеры мобильных устройств»

Минск 2026

ВВЕДЕНИЕ

Мобильные мессенджеры, социальные сети и сервисы электронной почты стали основным каналом коммуникации граждан и одновременно – одним из основных объектов преступных посягательств в сфере информационной безопасности. Завладев учетной записью, злоумышленник получает доступ к переписке, персональным данным и контактам владельца и использует аккаунт для рассылки мошеннических сообщений от его имени, вымогательства и дальнейшего распространения вредоносного программного обеспечения.

Значительная часть таких случаев связана не с техническим взломом, а с методами социальной инженерии: гражданину звонят или пишут от имени службы поддержки, банка, оператора связи или правоохранительного органа и под различными предлогами выманивают одноразовый код подтверждения. Если учетная запись защищена только кодом из SMS, его разглашение означает утрату контроля над аккаунтом.

Двухфакторная аутентификация существенно снижает этот риск, поскольку для входа в аккаунт на новом устройстве, помимо кода из SMS или пароля, требуется дополнительный элемент, известный или доступный только владельцу. Включение данной функции относится к базовым мерам защиты информации, обладателем которой является гражданин, и соответствует положениям Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Понятие и виды факторов аутентификации

Аутентификация – проверка подлинности пользователя, пытающегося получить доступ к учетной записи. Двухфакторная аутентификация (2FA) – способ проверки, при котором пользователь подтверждает свою личность двумя независимыми факторами, относящимися к разным категориям:

– **фактор знания** – то, что знает только пользователь (пароль, PIN-код, облачный пароль);

– **фактор владения** – то, чем располагает только пользователь (телефон с SIM-картой, приложение-аутентификатор, аппаратный ключ, доверенное устройство);

– **биометрический фактор** – физиологические признаки пользователя (отпечаток пальца, изображение лица).

В различных сервисах функция может называться «двухфакторная аутентификация», «двухэтапная проверка», «подтверждение входа», «облачный пароль», «двойная защита». Независимо от названия, ее назначение одинаково – исключить возможность входа в аккаунт по одному лишь коду из SMS.

1.2 Способы получения второго фактора

Способы подтверждения различаются по степени защищенности (в порядке ее убывания):

1. **Ключи доступа (passkeys) и аппаратные ключи** – не могут быть перехвачены или переданы мошеннику по телефону.

2. **Приложения-аутентификаторы** (Google Authenticator, Microsoft Authenticator, Яндекс Ключ и аналогичные) – генерируют одноразовые коды на устройстве без использования сети оператора связи.

3. **Облачный пароль или PIN-код** – известен только владельцу и не передается по каналам связи.

4. **Коды из SMS** – наименее защищенный способ: уязвим к перевыпуску SIM-карты, перехвату и выманиванию методами социальной инженерии.

1.3 Общие правила безопасности

При использовании двухфакторной аутентификации необходимо соблюдать следующие правила:

1. Никому не сообщать коды подтверждения, пароли и PIN-коды, в том числе лицам, представляющимся сотрудниками службы поддержки, банка, оператора связи или правоохранительных органов. Такие организации не запрашивают коды подтверждения.

2. Использовать для облачного пароля и PIN-кода уникальные комбинации, не совпадающие с другими паролями и не связанные с датами рождения, номерами телефонов и т. п.

3. Привязывать к аккаунту резервную электронную почту, доступ к которой также защищен двухфакторной аутентификацией.

4. Сохранять резервные коды восстановления на бумажном носителе или в защищенном хранилище отдельно от мобильного устройства.

5. По возможности использовать приложение-аутентификатор или ключ доступа вместо SMS.

6. Регулярно проверять перечень активных сеансов и подключенных устройств и завершать неизвестные.

7. Не устанавливать приложения из неофициальных источников и не переходить по ссылкам из сообщений с просьбой «подтвердить аккаунт» или «проголосовать».

Примечание – Наименования пунктов меню приведены по состоянию на октябрь 2026 г. и могут незначительно отличаться в зависимости от версии приложения и операционной системы (Android или iOS).

2 ПАМЯТКИ-АЛГОРИТМЫ ПО УСТАНОВКЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

2.1 Telegram

В Telegram второй фактор реализован в виде облачного пароля, который запрашивается при входе в аккаунт на новом устройстве после ввода кода из SMS.

Таблица 1 – Алгоритм включения функции «облачный пароль (двухэтапная аутентификация)» в Telegram

№	Действие	Путь в интерфейсе / ожидаемый результат
1	Открыть настройки приложения	Главный экран → «Настройки»
2	Перейти в раздел конфиденциальности	«Конфиденциальность»
3	Выбрать функцию облачного пароля	«Облачный пароль» (в ряде версий – «Двухэтапная аутентификация»)
4	Задать пароль	«Задать пароль» → дважды ввести надежный пароль
5	Указать подсказку	Подсказка не должна содержать сам пароль или прямо указывать на него
6	Привязать электронную почту для восстановления	Ввести адрес электронной почты → ввести код подтверждения из письма. Результат: облачный пароль включен

Дополнительно рекомендуется: проверить перечень активных сеансов («Настройки» → «Устройства») и завершить незнакомые; при наличии – настроить вход с использованием ключа доступа.

Памятки-алгоритмы в виде инфографики для устройств на платформах iOS и Android приведены в приложении А (рисунки А.1, А.2).

2.2 WhatsApp

Двухшаговая проверка в WhatsApp предусматривает ввод шестизначного PIN-кода при регистрации номера телефона на новом устройстве.

Таблица 2 – Алгоритм включения функции «двухшаговая проверка» в WhatsApp

№	Действие	Путь в интерфейсе / ожидаемый результат
1	Открыть настройки приложения	«Настройки» (iOS – вкладка внизу экрана; Android – меню «⋮»)
2	Перейти в раздел аккаунта	«Аккаунт»
3	Выбрать двухшаговую проверку	«Двухшаговая проверка» → «Включить»
4	Задать PIN-код	Ввести и подтвердить шестизначный PIN-код

№	Действие	Путь в интерфейсе / ожидаемый результат
5	Указать электронную почту	Адрес используется для сброса PIN-кода при его утрате
6	Подтвердить адрес	Ввести код из письма. Результат: двухшаговая проверка включена

Дополнительно рекомендуется: настроить ключ доступа («Аккаунт» → «Ключи доступа»); проверить раздел «Связанные устройства» и выйти с неизвестных устройств.

Памятка-алгоритм в виде инфографики приведена в приложении Б.

2.3 Viber

В Viber защита учетной записи обеспечивается PIN-кодом, который запрашивается при активации аккаунта на новом устройстве.

Таблица 3 – Алгоритм включения функции «PIN-код защиты учетной записи» в Viber

№	Действие	Путь в интерфейсе / ожидаемый результат
1	Открыть меню приложения	«Еще» (☰) → «Настройки»
2	Перейти в раздел учетной записи	«Учетная запись»
3	Выбрать функцию защиты	«Двухэтапная проверка» / «Защита аккаунта»
4	Задать PIN-код	Ввести и подтвердить шестизначный PIN-код
5	Указать и подтвердить электронную почту	Перейти по ссылке из письма. Результат: защита учетной записи включена

Дополнительно рекомендуется: проверить раздел «Компьютеры и планшеты» и деактивировать неизвестные устройства.

Памятка-алгоритм в виде инфографики приведена в приложении В.

2.4 ВКонтакте (VK ID)

Учетная запись VK ID используется для входа во ВКонтакте и связанные сервисы, поэтому ее защита распространяется на все эти сервисы одновременно.

Таблица 4 – Алгоритм включения функции «подтверждение входа» в ВКонтакте

№	Действие	Путь в интерфейсе / ожидаемый результат
1	Открыть управление учетной записью	Профиль → «☰» → «Управление VK ID»
2	Перейти в раздел безопасности	«Безопасность и вход»
3	Включить подтверждение входа	«Подтверждение входа» (защита входа)
4	Подтвердить действие	Ввести код из SMS или уведомления

№	Действие	Путь в интерфейсе / ожидаемый результат
5	Выбрать способ получения кодов	SMS или приложение-аутентификатор (предпочтительно)
6	Сохранить резервные коды	Записать и хранить отдельно от телефона. Результат: подтверждение входа включено

Памятка-алгоритм в виде инфографики приведена в приложении Г.

2.5 Instagram

Настройка безопасности Instagram осуществляется через единый Центр аккаунтов, общий для сервисов компании-разработчика.

Таблица 5 – Алгоритм включения функции «двухфакторная аутентификация» в Instagram

№	Действие	Путь в интерфейсе / ожидаемый результат
1	Открыть меню профиля	Профиль → «☰» → «Центр аккаунтов»
2	Перейти в раздел безопасности	«Пароль и безопасность»
3	Выбрать двухфакторную аутентификацию	«Двухфакторная аутентификация» → выбрать аккаунт
4	Выбрать способ защиты	Приложение аутентификации (рекомендуется), SMS или WhatsApp
5	Подтвердить настройку	Ввести полученный код
6	Сохранить резервные коды	Хранить отдельно от телефона. Результат: 2FA включена

2.6 TikTok

TikTok предусматривает выбор не менее двух способов подтверждения входа.

Таблица 6 – Алгоритм включения функции «двухэтапная проверка» в TikTok

№	Действие	Путь в интерфейсе / ожидаемый результат
1	Открыть настройки	«Профиль» → «☰» → «Настройки и конфиденциальность»
2	Перейти в раздел безопасности	«Безопасность и разрешения» (в ряде версий – «Безопасность»)
3	Выбрать двухэтапную проверку	«Двухэтапная проверка»
4	Отметить способы подтверждения	Не менее двух: SMS, электронная почта, приложение-аутентификатор
5	Включить функцию	«Включить» → подтвердить паролем. Результат: двухэтапная проверка включена

Памятка-алгоритм в виде инфографики приведена в приложении Е.

2.7 Apple ID (iPhone, iPad)

Для большинства современных учетных записей Apple ID двухфакторная аутентификация включена по умолчанию; необходимо проверить ее статус и актуальность доверенного номера.

Таблица 7 – Алгоритм включения функции «двухфакторная аутентификация» в Apple ID

№	Действие	Путь в интерфейсе / ожидаемый результат
1	Открыть настройки учетной записи	«Настройки» → [имя пользователя]
2	Перейти в раздел безопасности	«Вход и безопасность» (ранее – «Пароль и безопасность»)
3	Включить функцию	«Включить двухфакторную аутентификацию» → «Продолжить»
4	Указать доверенный номер телефона	Ввести номер, к которому имеется постоянный доступ
5	Подтвердить настройку	Ввести код подтверждения. Результат: 2FA включена

Дополнительно рекомендуется: включить функцию «Защита украденного устройства» («Настройки» → «Face ID и код-пароль»).

Памятка-алгоритм в виде инфографики приведена в приложении Ж.

3 ПОРЯДОК ДЕЙСТВИЙ ПРИ КОМПРОМЕТАЦИИ УЧЕТНОЙ ЗАПИСИ

При утрате доступа к аккаунту или обнаружении признаков его несанкционированного использования (сообщения, которые владелец не отправлял, уведомления о входе с неизвестного устройства, изменение пароля или привязанного номера) рекомендуется:

1. Незамедлительно воспользоваться официальной процедурой восстановления доступа, предусмотренной сервисом (форма восстановления, обращение в службу поддержки через приложение или официальный сайт).
2. Предупредить родственников, друзей и коллег о том, что от имени владельца могут поступать просьбы о переводе денежных средств, сообщении кодов или переходе по ссылкам.
3. Сменить пароли на связанных сервисах (электронная почта, банковские приложения, иные аккаунты с аналогичным паролем) и включить на них двухфакторную аутентификацию.
4. Завершить все активные сеансы и отключить неизвестные устройства после восстановления доступа.

ЗАКЛЮЧЕНИЕ

Включение двухфакторной аутентификации занимает несколько минут, не требует специальных знаний и при этом существенно снижает вероятность несанкционированного доступа к учетным записям граждан. Использование наглядных памяток-алгоритмов в профилактической работе позволяет повысить уровень цифровой грамотности населения и сократить количество преступлений, совершаемых с использованием методов социальной инженерии.

ПРИЛОЖЕНИЕ А
(справочное)

ПАМЯТКА-АЛГОРИТМ ДЛЯ TELEGRAM

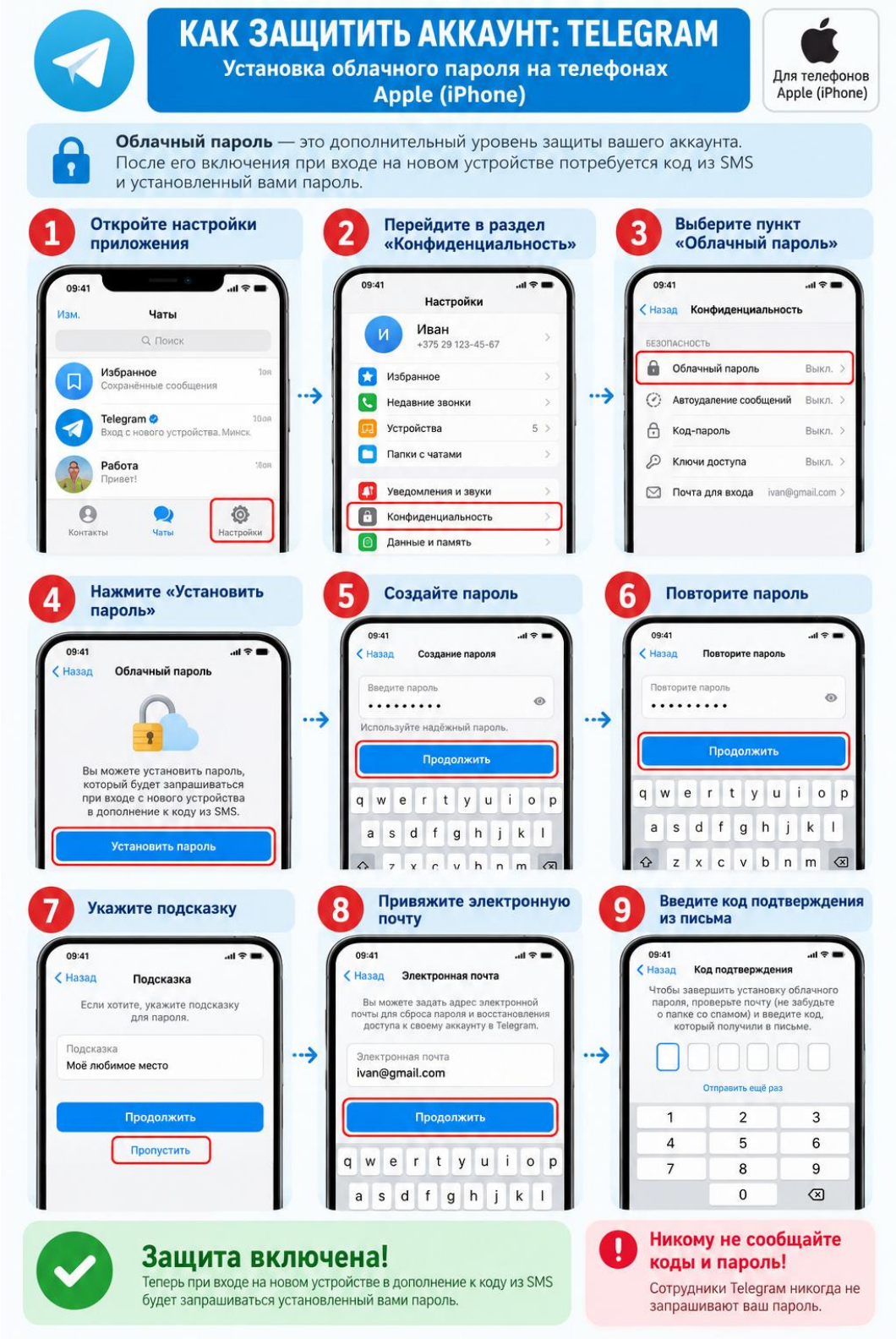


Рисунок А.1 – Включение облачного пароля в Telegram (iOS)



Рисунок А.2 – Включение облачного пароля в Telegram (Android)

ПРИЛОЖЕНИЕ Б
(справочное)

ПАМЯТКА-АЛГОРИТМ ДЛЯ WHATSAPP

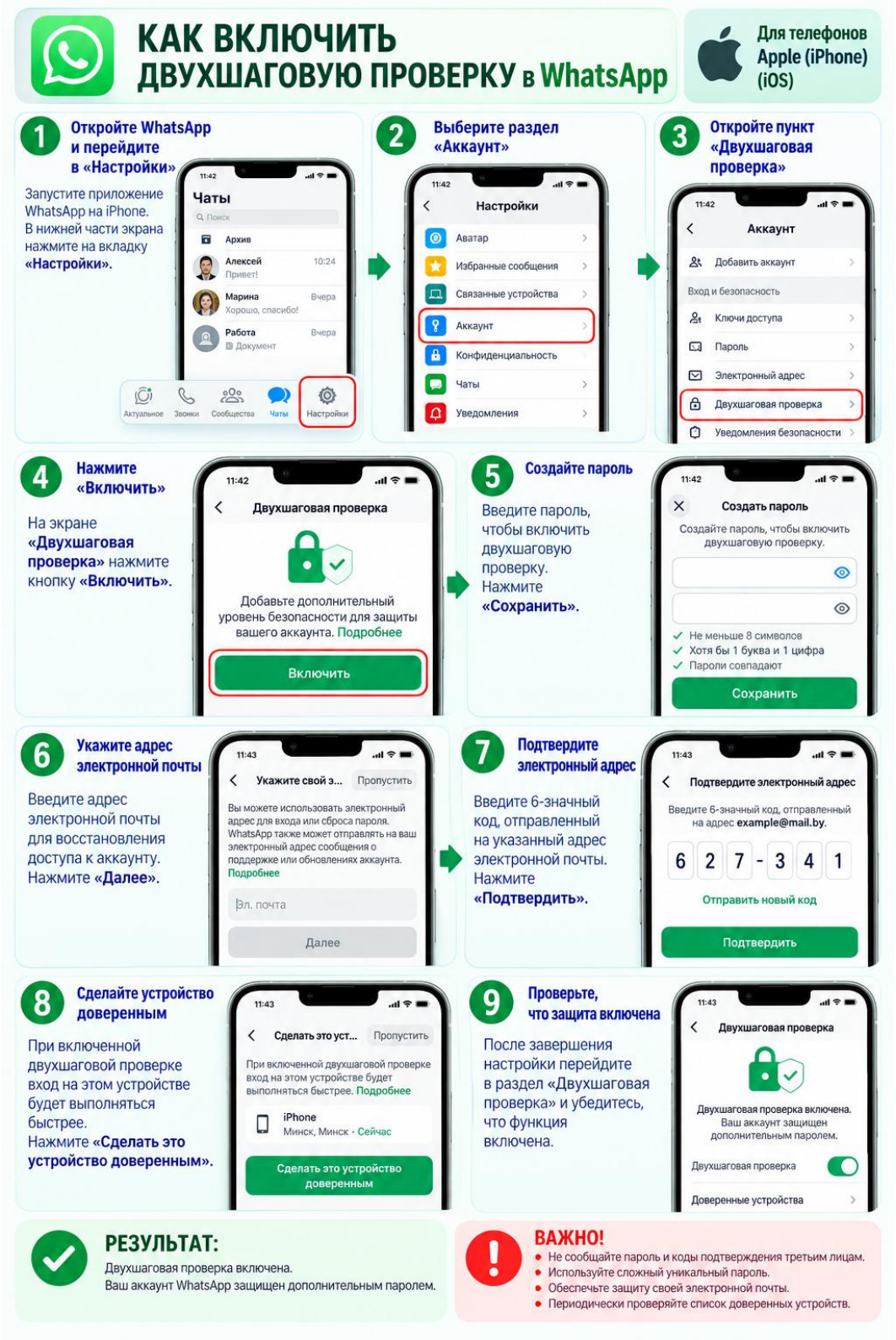


Рисунок Б.1 – Включение двухшаговой проверки в WhatsApp (iOS)

ПРИЛОЖЕНИЕ В
(справочное)

ПАМЯТКА-АЛГОРИТМ ДЛЯ VIBER

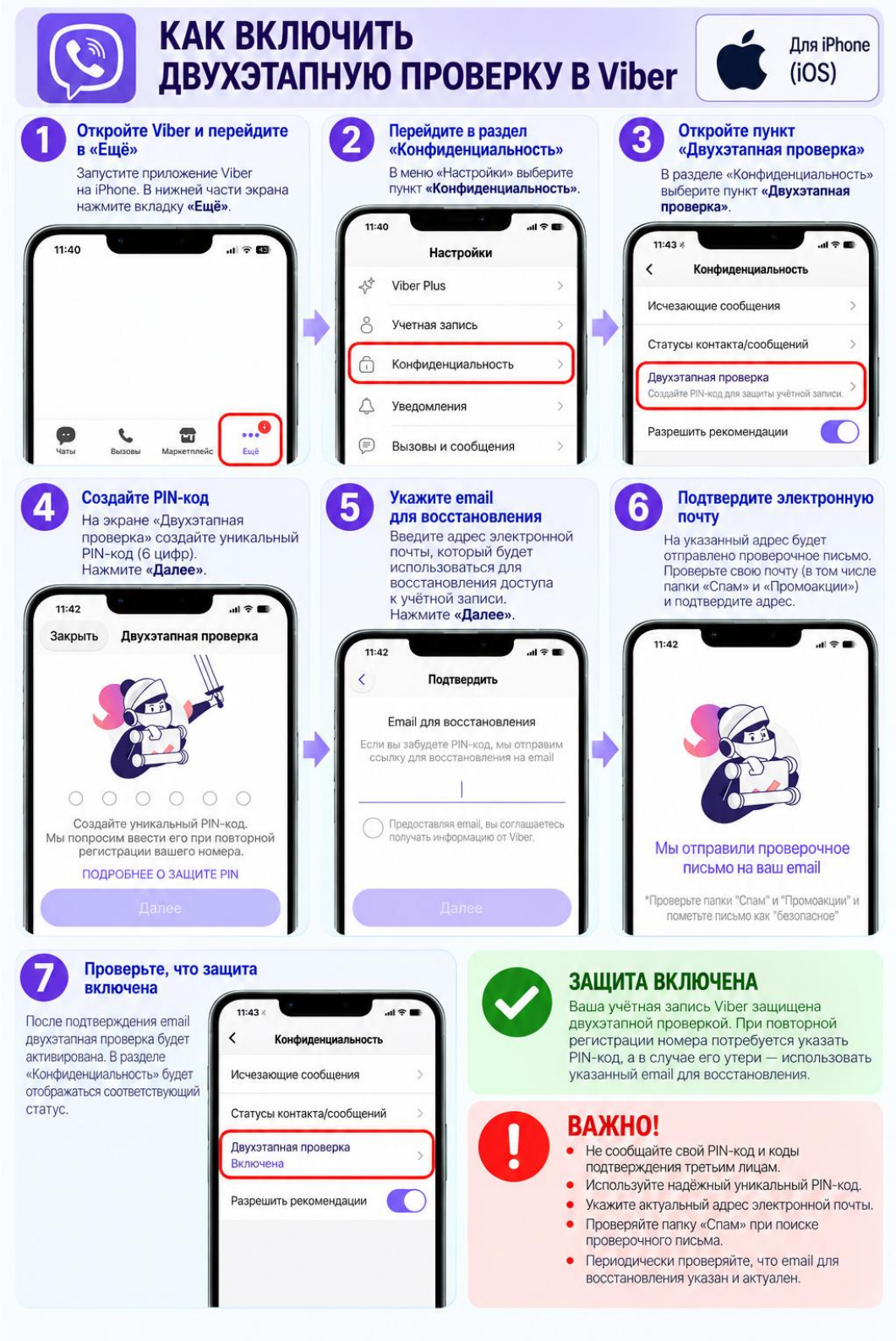


Рисунок В.1 – Включение двухэтапной проверки в Viber (iOS)

ПРИЛОЖЕНИЕ Г
(справочное)

ПАМЯТКА-АЛГОРИТМ ДЛЯ ВКОНТАКТЕ

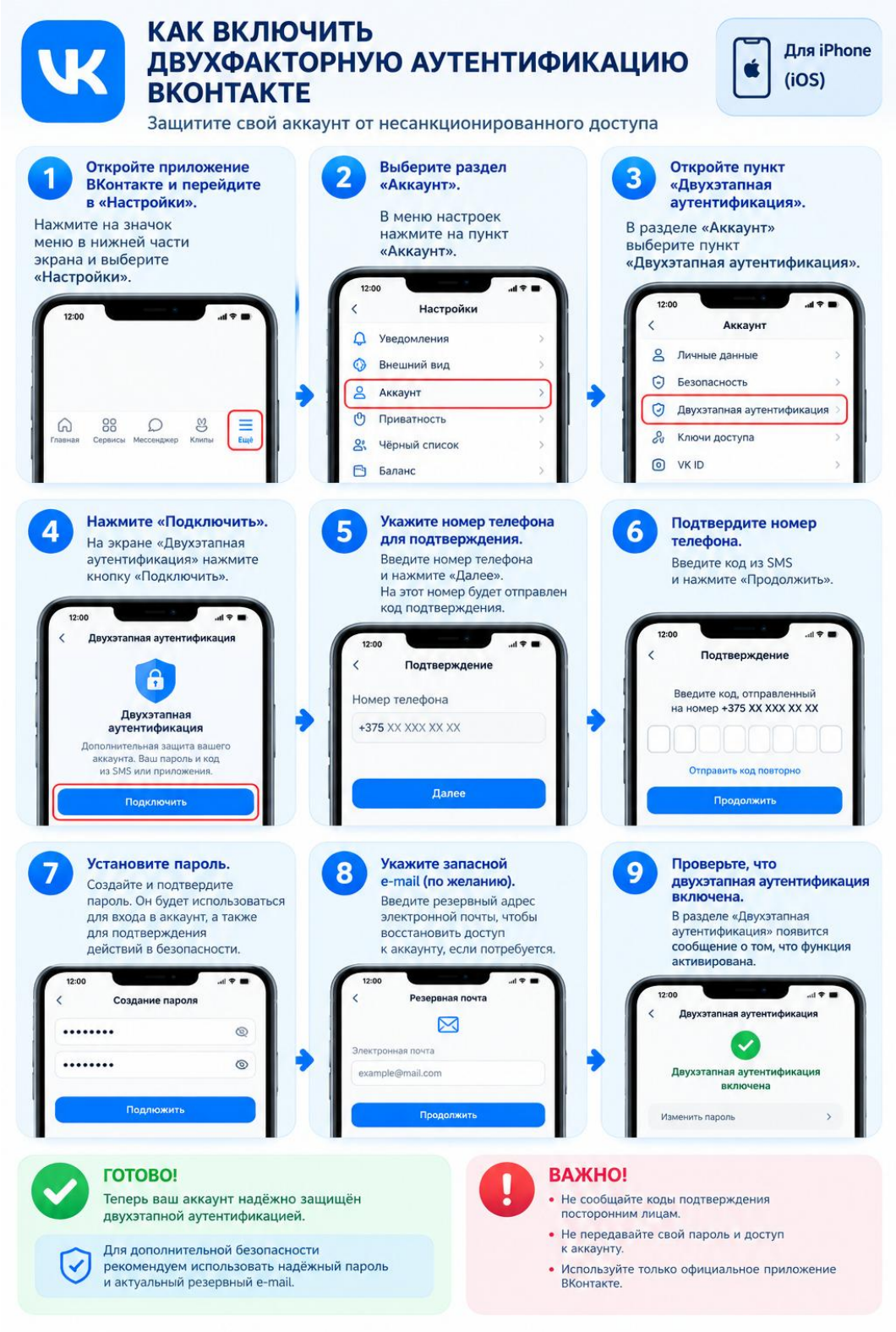


Рисунок Г.1 – Включение подтверждения входа во ВКонтакте

ПРИЛОЖЕНИЕ Д
(справочное)

ПАМЯТКА-АЛГОРИТМ ДЛЯ INSTAGRAM

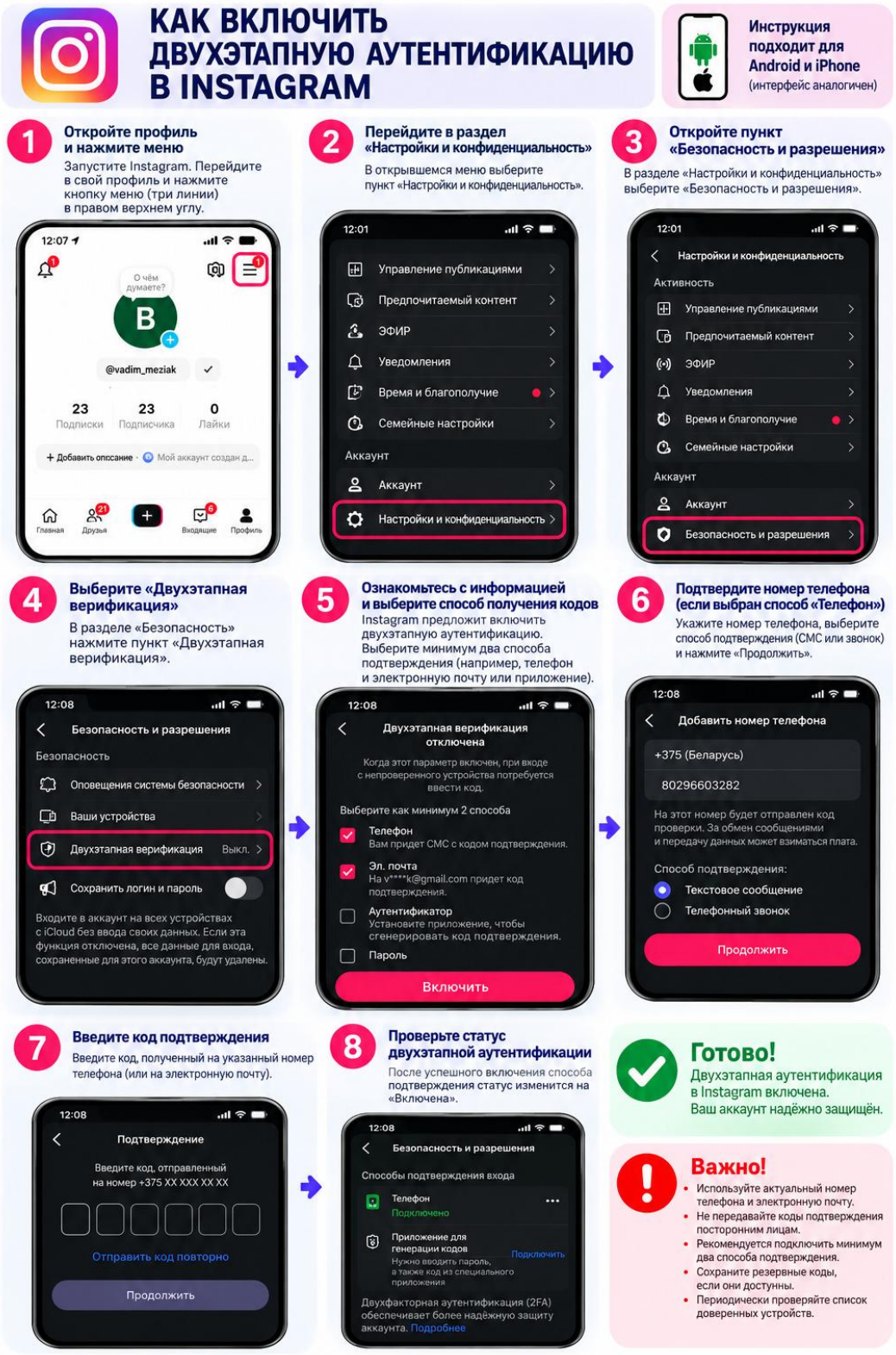


Рисунок Д.1 – Включение двухфакторной аутентификации в Instagram

ПРИЛОЖЕНИЕ Е
(справочное)

ПАМЯТКА-АЛГОРИТМ ДЛЯ TIKTOK

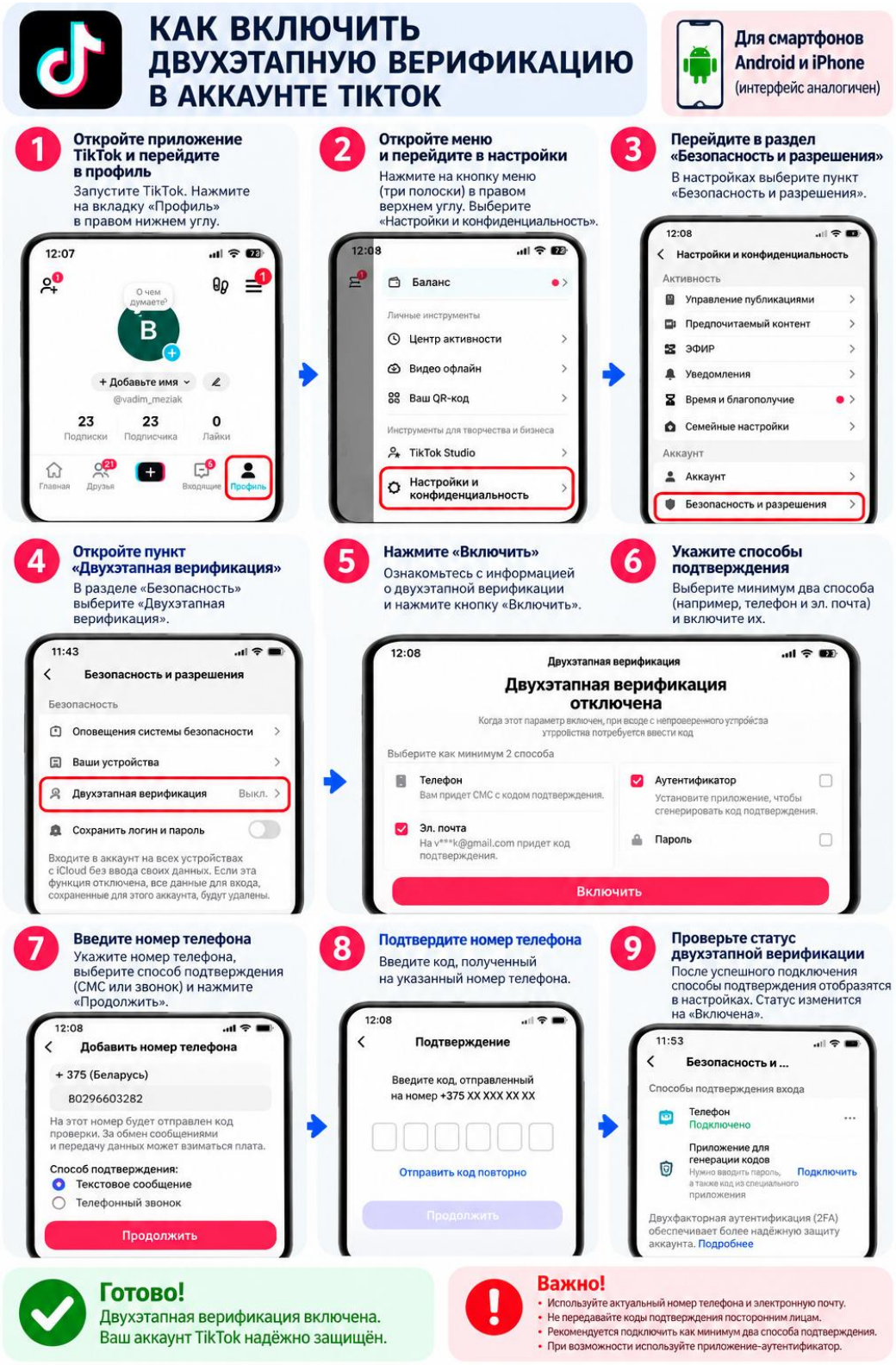


Рисунок Е.1 – Включение двухэтапной проверки в TikTok

ПРИЛОЖЕНИЕ Ж
(справочное)

ПАМЯТКА-АЛГОРИТМ ДЛЯ APPLE ID

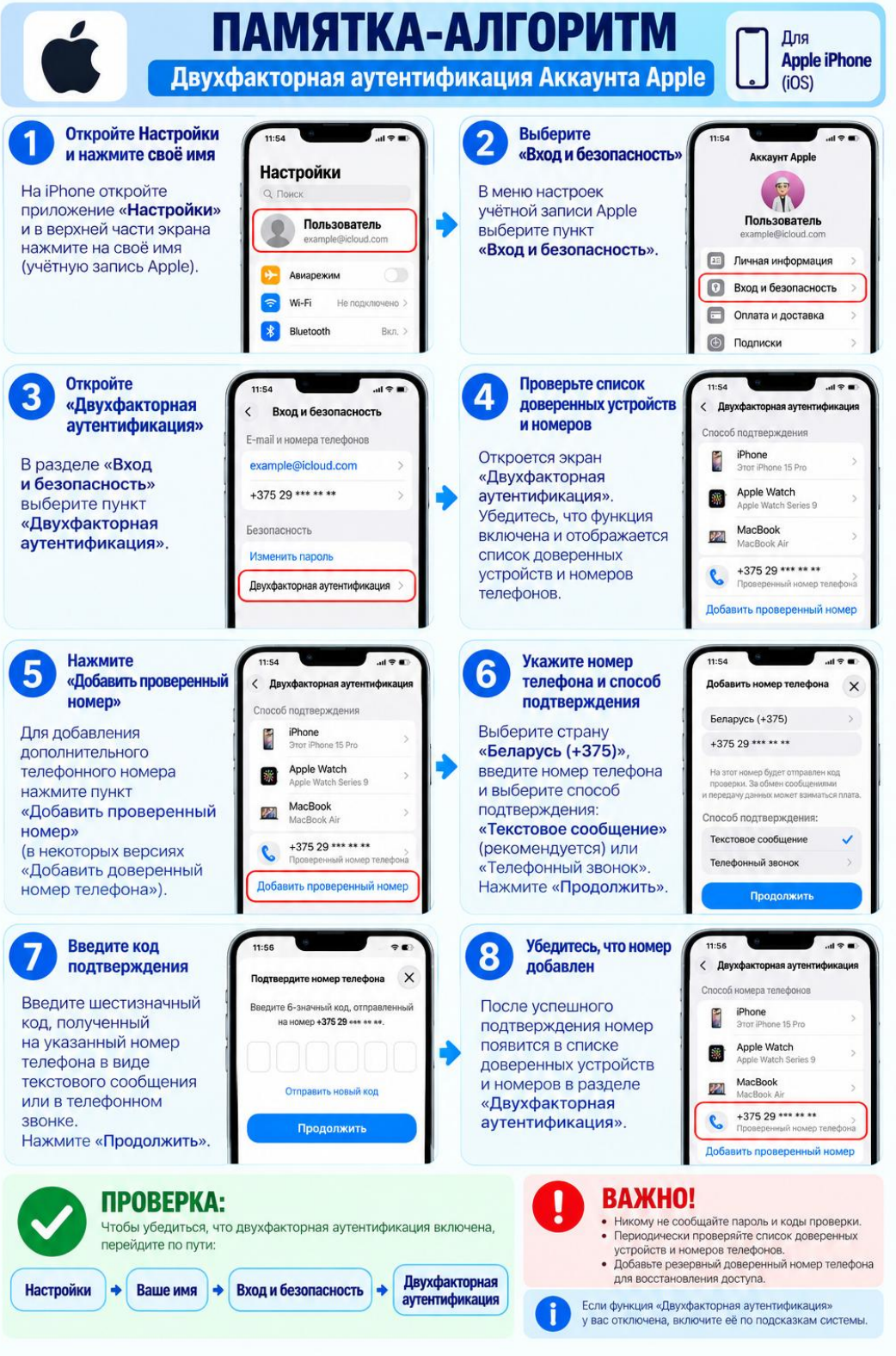


Рисунок Ж.1 – Включение двухфакторной аутентификации в Apple ID (iOS)