

РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО)

18.05.2020 г.

г. Махачкала

**«Клиентам системы
дистанционного банковского
обслуживания «iBank2»»**

В связи с необходимостью снижения рисков воздействия вредоносного кода и повышения уровня безопасности при работе с системой дистанционного банковского обслуживания «iBank2» (Интернет-банком) Комитет по информационной безопасности РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО) рекомендует клиентам применять в своей работе организационные меры защиты информации, указанные в Приложениях 1 и 2 к данному письму. В случае возникновения вопросов по применению организационных мер защиты просим Вас позвонить в Комитет по информационной безопасности по номеру 8 (8722) 51-70-44.

Председатель Правления



К.А.Абдурахманов

**ПРАВИЛА БЕЗОПАСНОСТИ ПРИ РАБОТЕ
КЛИЕНТОВ С СИСТЕМОЙ ДБО «iBANK2»**

Для безопасной работы в системе ДБО «iBank2» клиентам необходимо придерживаться следующих правил:

- 1) usb-ключи iBank2 Key хранить в месте, не доступном посторонним лицам;
- 2) храните в тайне пароль доступа к usb-ключу iBank2 Key, исключите запись пароля на стикерах, на самом usb-ключе. **НИКОМУ НЕ СООБЩАЙТЕ** пароль по телефону, даже сотрудникам РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО);
- 3) пароль должен быть известен **ТОЛЬКО** владельцу usb-ключа;
- 4) используйте в работе с системой ДБО «iBank2» двухфакторную аутентификацию при осуществлении платежей (по PIN-коду usb-ключа и одноразовому оповещению через приложение «Весточка» компании «БИФИТ», установленному на телефоне). При этом, доступ к usb-ключу и к телефону, на котором установлено приложение «Весточка» компании «БИФИТ», **ДОЛЖЕН БЫТЬ ОГРАНИЧЕН** только лицом, уполномоченным совершать платежи клиента (владельцем ключа);
- 5) Рекомендуется совершать платежи и работать с системой ДБО «iBank2» на **ОДНОМ** выделенном компьютере **ТОЛЬКО** для работы с Интернет-банком. На отделенном от локальной сети компьютере должна проводиться работа **ТОЛЬКО** с системой ДБО «iBank2», иных операций на этом компьютере **НЕ** рекомендуется совершать;
- 6) На отделенном от локальной сети компьютере должен быть доступ в интернет **ТОЛЬКО** для системы ДБО «iBank2», **ИНЫХ ИНТЕРНЕТ-СОЕДИНЕНИЙ** на этом компьютере **НЕ ДОЛЖНО БЫТЬ**. Для этого рекомендуется настроить сетевой экран с разрешающим правилом доступа к системе ДБО «iBank2» (http://psib.ru/*, <http://psib.ru/internet-bank.php>, <https://ibank.psib.ru:9443/ibank2/#/>) и запрещающим правилом на все остальные сетевые интернет-соединения;
- 7) usb-ключ iBank2 Key должен быть подключен к usb-порту компьютера **ТОЛЬКО** во время совершения платежа по системе ДБО «iBank2». **ПОСЛЕ** совершения платежа usb-ключ iBank2 Key необходимо **ОТСОЕДИНИТЬ** от usb-порта. **ПОДКЛЮЧЕНИЕ** usb-ключа iBank2 Key к компьютеру необходимо осуществлять только **ПО МЕРЕ НЕОБХОДИМОСТИ** совершить платеж через систему ДБО «iBank2»;
- 8) на компьютере, который используется в работе с системой ДБО «iBank2», **НЕ ДОЛЖНО БЫТЬ** установленных **ПОСТОРОННИХ ПРОГРАММ** (только драйвера операционной системы, драйвера на оборудование, драйвера на настройку системы ДБО «iBank2»);
- 9) используйте только лицензионное антивирусное программное обеспечение (антивирус). Антивирусное программное обеспечение (антивирус) должен быть установлен на каждом компьютере в локальной сети;
- 10) необходимо регулярно устанавливать обновления антивирусных баз на антивирусное программное обеспечение и обновления на операционную систему;
- 11) регулярно **ПРОВЕРЯЙТЕ** компьютер на **ВИРУСЫ** (вредоносный код) антивирусным программным обеспечением (антивирусом), не реже 1 раза в неделю;

12) при работе с электронной почтой **НЕ ОТКРЫВАЙТЕ** письма, полученные от **НЕИЗВЕСТНЫХ** отправителей, и вложения к ним. **НЕ ПЕРЕХОДИТЕ** по ссылкам из таких писем. Порядок работы с электронной почтой указан в Приложении 2 к письму;

13) на компьютере с системой ДБО «iBank2» **НЕ ИСПОЛЬЗУЙТЕ** права **АДМИНИСТРАТОРА** операционной системы семейства Windows без крайней необходимости. Работа на компьютере с Интернет-банком должна осуществляться **ПОД ПРАВАМИ** локального **ПОЛЬЗОВАТЕЛЯ**. В повседневной практике входите в операционную систему как **ЛОКАЛЬНЫЙ ПОЛЬЗОВАТЕЛЬ** без прав администратора;

14) при работе в Интернете **НЕ СОГЛАШАЙТЕСЬ** на установку дополнительных программ;

15) **НЕ СОХРАНЯЙТЕ** PIN-код usb-ключа iBank2 Key на общедоступных компьютерах и на своем компьютере **В ВИДЕ ТЕКСТОВЫХ ФАЙЛОВ** (в форматах txt, doc, docx, rtf, в иных текстовых форматах);

16) **НЕ ПОДКЛЮЧАЙТЕ** к usb-портам без служебной необходимости usb-flash накопителя (флешки). В случае рабочей необходимости после подключения флешку необходимо проверить антивирусным программным обеспечением (антивирусом);

17) при входе в систему клиентам рекомендовано обращать внимание на журнал сеансов, ведущихся в системе ДБО «iBank2», в котором отражаются дата, время последних операций, а также ip-адреса, с которых был осуществлен вход в систему;

18) **В КОНЦЕ РАБОЧЕГО ДНЯ** в случае отсутствия необходимости в работе с Интернет-банком необходимо **ВЫКЛЮЧИТЬ** компьютер с системой ДБО «iBank2».

ПОРЯДОК РАБОТЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ НА КОМПЬЮТЕРЕ С СИСТЕМОЙ ДБО «IBANK2»

В случае использования электронной почты в работе с контрагентами в целях обеспечения защиты информации от утечки, воздействия вредоносного кода (вирусов) клиентам необходимо придерживаться следующих правил:

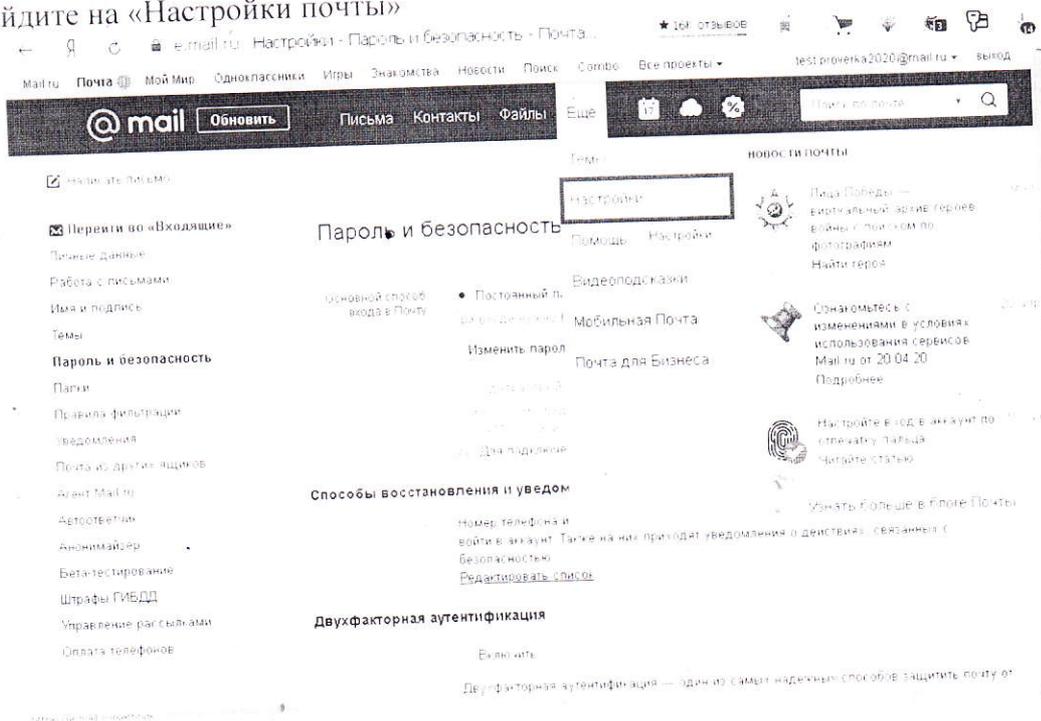
1. Пароль на электронную почту должен соответствовать не менее трем категориям сложности: обязательное наличие букв, цифр, длина пароля не менее 8 символов. Рекомендуется также применять в пароле специальные символы, которые не являются ни буквой, ни цифрой (например, !@#%\$%^&), если почта поддерживает возможность ввода специальных символов. Для надежного способа запомнить длинный пароль необходимо с английской раскладкой клавиатуры набирать пароль на русском языке (например, для набора пароля «безопасность» на английской раскладке он будет выглядеть как «trjgfcyujcnn»).

2. Для защиты почты от взлома рекомендуется воспользоваться двухфакторной аутентификацией (2FA) – дополнительный уровень безопасности, позволяющий войти на почту с использованием двух факторов: 1) обычного пароля для входа на почту 2) временного пароля, который можно получить через SMS-уведомление по телефону.

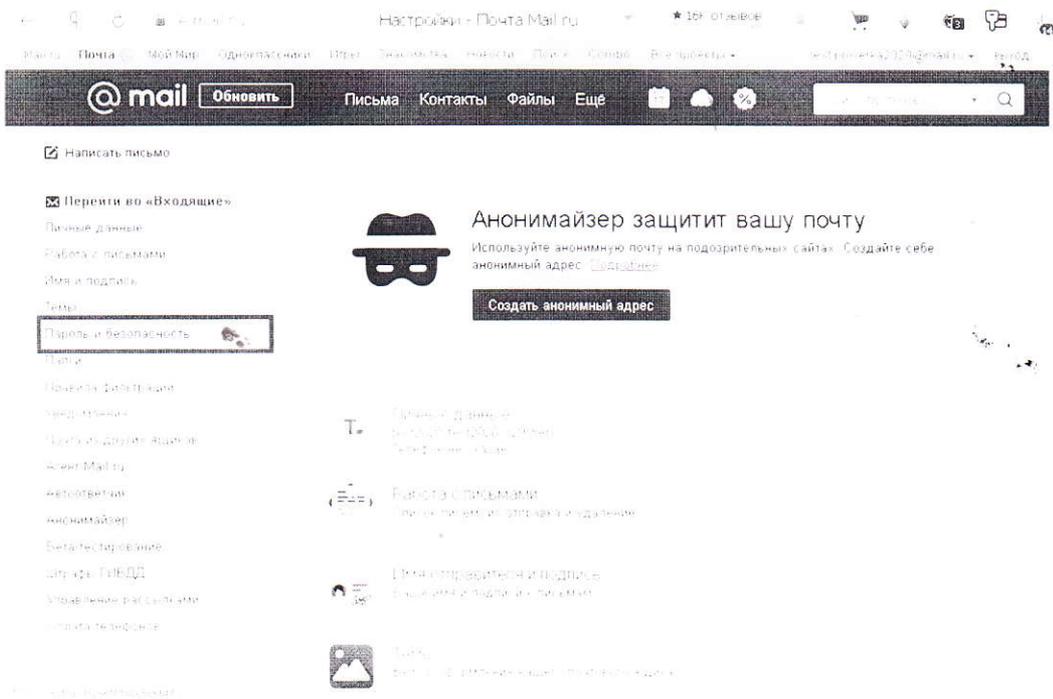
2.1. Настройка двухфакторной аутентификации (2FA) на mail.ru

Для того чтобы включить двухфакторную аутентификацию:

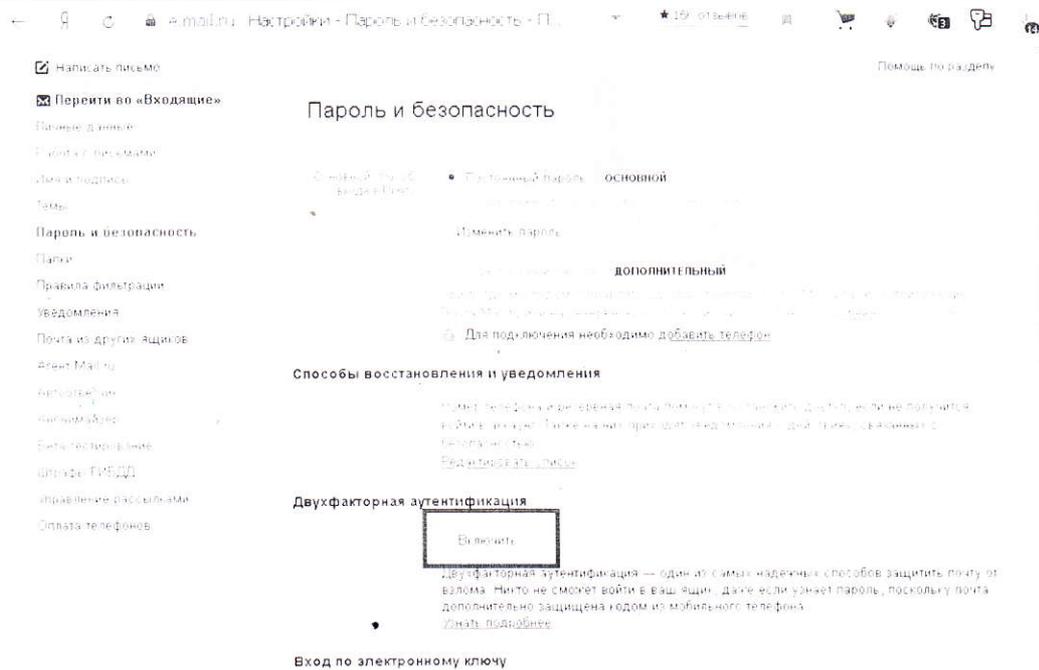
1. Перейдите на «Настройки почты»



2. Выберите пункт «Пароль и безопасность»



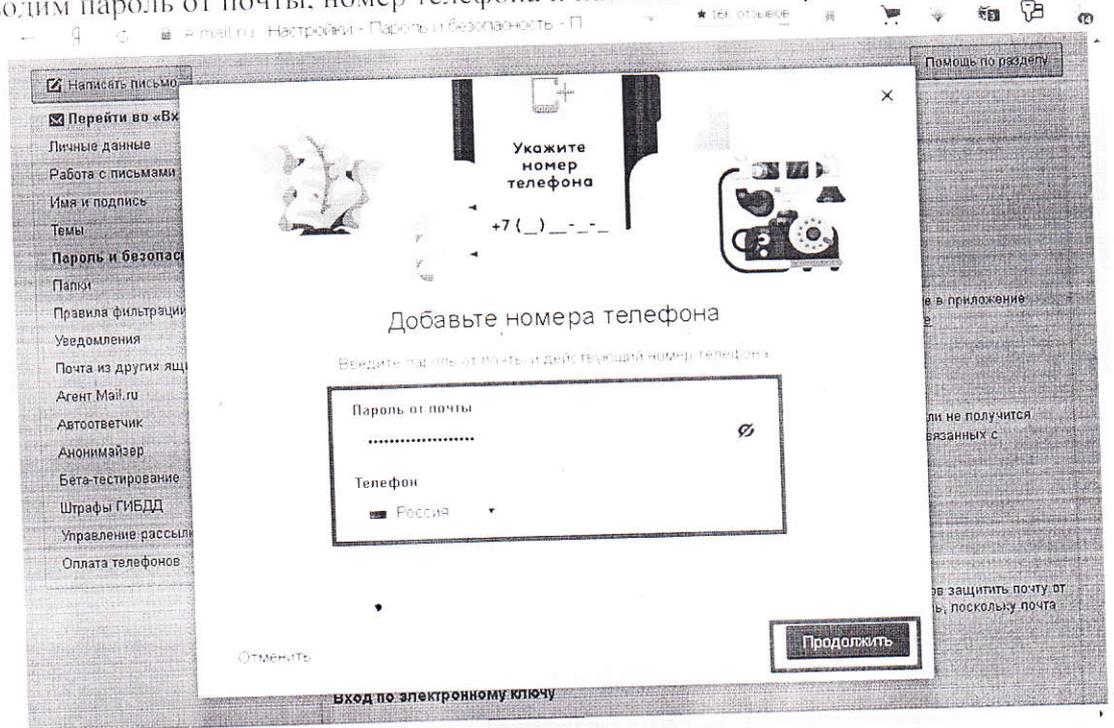
3. В разделе «двухфакторная аутентификация» нажмите «Включить»



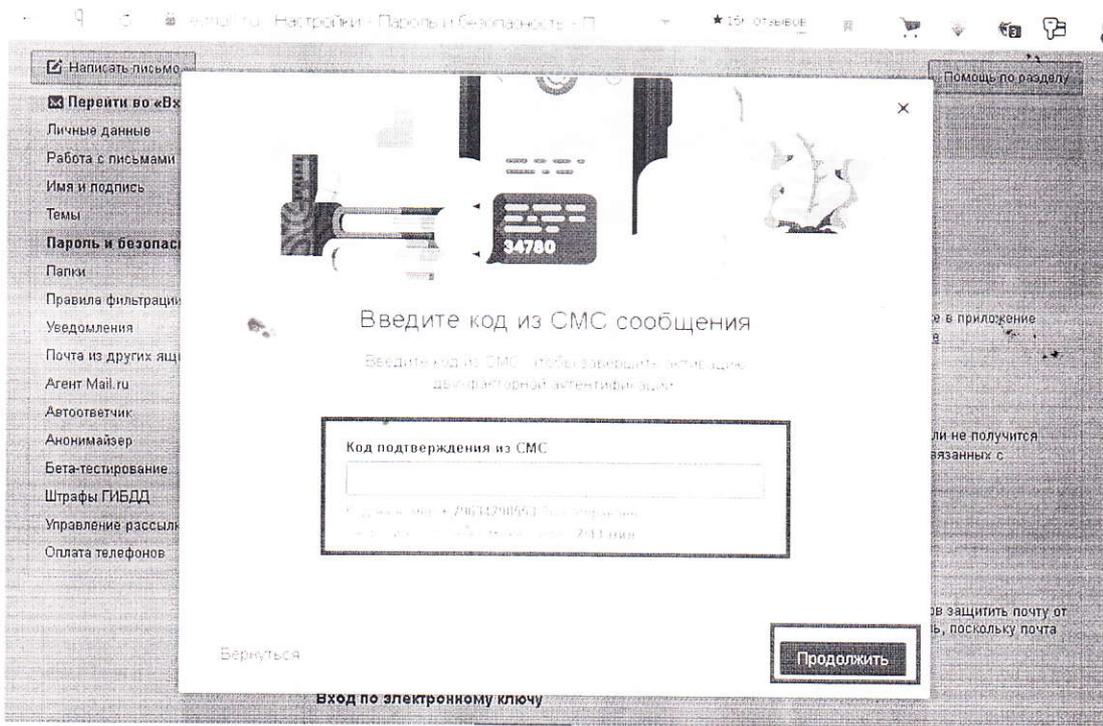
4. Внизу окна нажимаем на «Хочу получать код по СМС»



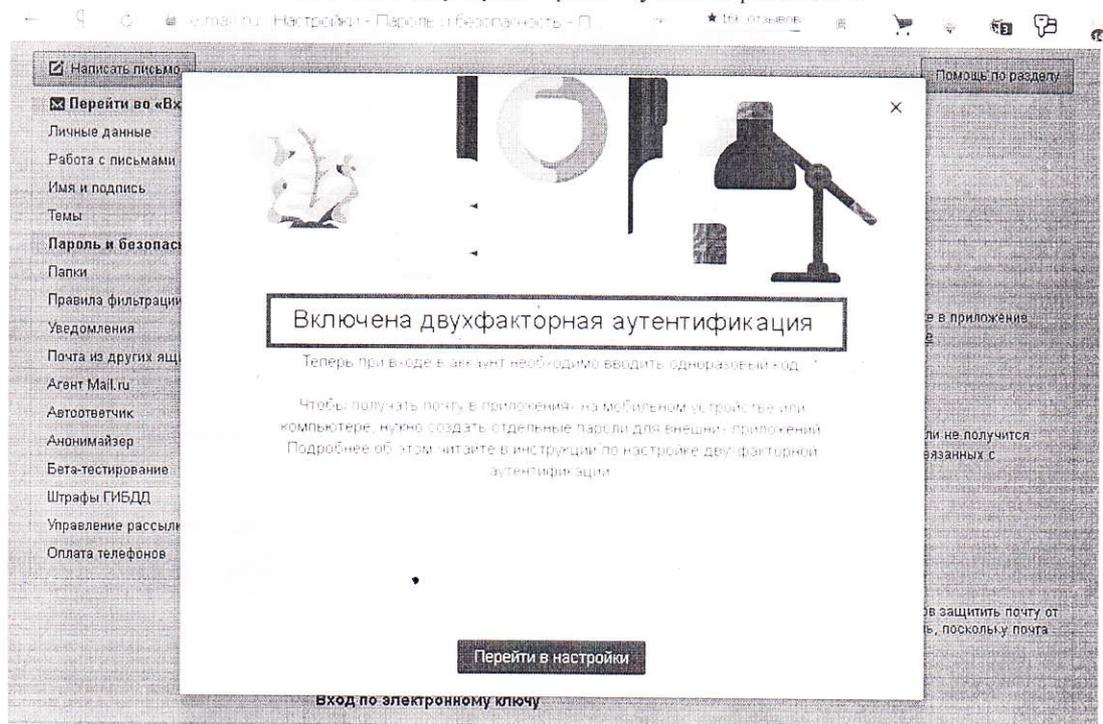
5. Вводим пароль от почты, номер телефона и нажимаем на «Продолжить»



6. Вводим полученный в SMS-уведомлении код подтверждения, затем нажимаем на «Продолжить»



7. Выйдет сообщение «Включена двухфакторная аутентификация»



8. Для проверки настроек по двухфакторной аутентификации выходим с почты и заново пробуем войти в почту.



Поиск



Почта



Новости

test proverk @mail.ru

Ввести пароль →



Запомнить [Забыли пароль?](#)

Средни

Аномали

Ведущи

Туриста

Создать почту



Облако

9. Затем необходимо ввести код подтверждения из SMS-уведомления. Галочку «Не спрашивать для этого устройства» рекомендуется убрать.

Вход в Mail.ru

Код подтверждения отправлен на номер +7 (963) 429-**-**

Код подтверждения

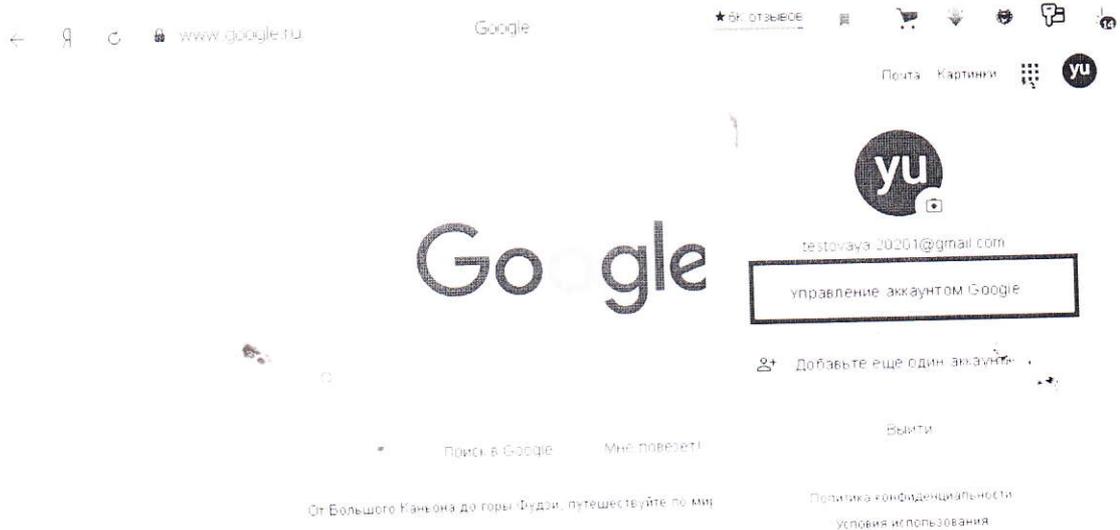
Не спрашивать для этого устройства

Войти

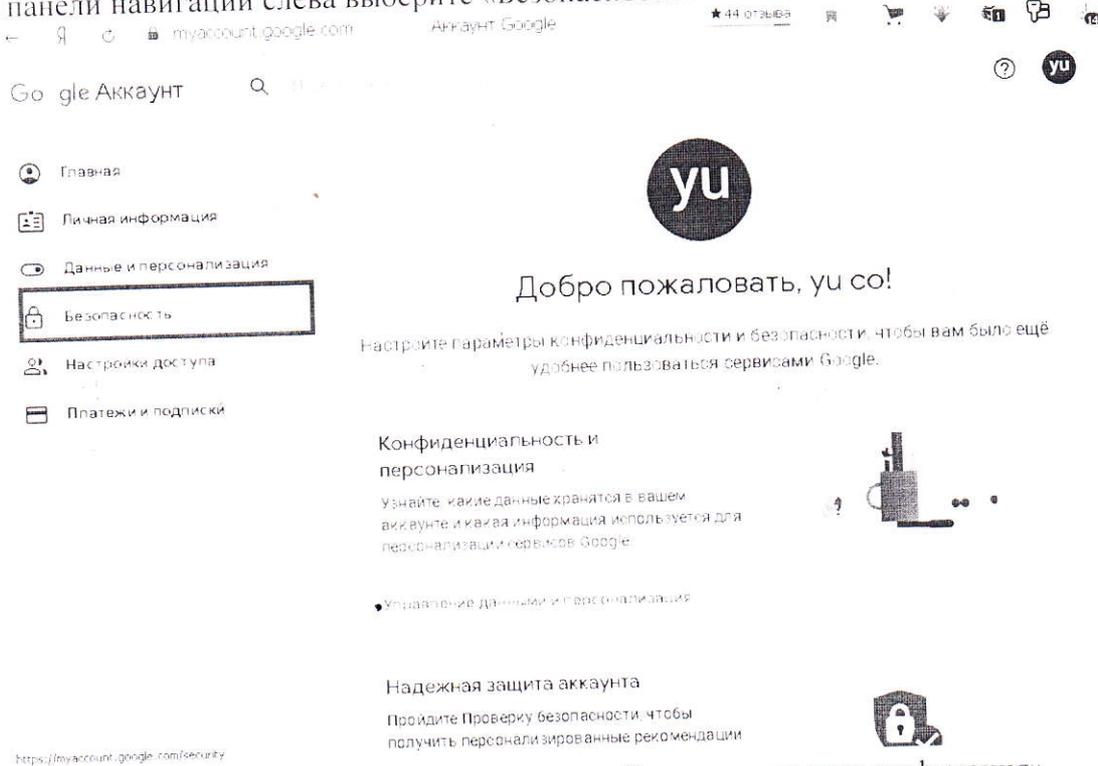
[Проблемы со входом?](#)

2.2. Настройка двухфакторной аутентификации на почте gmail.com

1. Откройте страницу «Аккаунт Google»



2. На панели навигации слева выберите «Безопасность»



3. В разделе «Вход в аккаунт Google» нажмите «Двухэтапная аутентификация»

myaccount.google.com Аккаунт Google 44 отзыва

Google Аккаунт

- Главная
- Личная информация
- Данные и персонализация
- Безопасность
- Настройки доступа
- Платежи и подписки

Вход в аккаунт Google

Пароль Последнее изменение: 14.04

Вход в аккаунт с помощью телефона Выкл

Двухэтапная аутентификация Выкл

Способы подтверждения личности

Это нужно, чтобы при необходимости мы могли сообщить вам о подозрительной активности или убедиться, что в аккаунт входите именно вы.

Номер телефона 8 (963) 429 85 53

Резервный адрес электронной почты Добавьте адрес электронной почты

4. Выберите «Начать»

myaccount.google.com Двухэтапная аутентификация 44 отзыва

Google Аккаунт

← Двухэтапная аутентификация

Защитите свой аккаунт с помощью двухэтапной аутентификации

Каждый раз при входе в аккаунт Google вам нужно будет вводить пароль и код подтверждения. Подробнее

- 

Примите дополнительные меры безопасности

Введите пароль и уникальный код подтверждения, который был отправлен на ваш телефон.
- 

Не дайте злоумышленникам завладеть им

Даже если кто-то узнает ваш пароль, этого будет недостаточно, чтобы войти в ваш аккаунт.

НАЧАТЬ

[Политика конфиденциальности](#) · [Удаление использования](#) · [Справка](#)

5. Введите пароль от почты gmail.com

Google
you

testovaya.20201@gmail.com

Сначала подтвердите, что это ваш аккаунт

Введите пароль

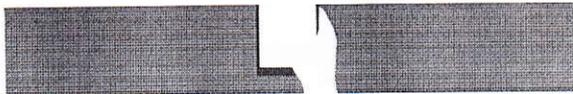
Забыли пароль?

Далее

6. Введите номер телефона в формате 9601234567, выбираем «SMS», нажимаем на кнопку «Далее»

Google Аккаунт

Двухэтапная аутентификация



Настройте телефон

Какой номер телефона вы хотите использовать?

Country code dropdown and phone number input field.

Google будет использовать это номер исключительно для защиты аккаунта. Не указывайте номер 0000000000. Мобильный оператор может взимать плату за передачу данных.

Как вы хотите получать коды?

SMS Телефонный звонок

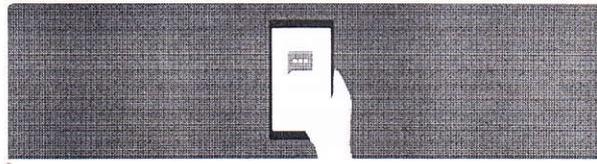
Не хотите получать коды с помощью SMS или голосового вызова? Выберите другой способ

Шаг 1 из 3

Далее

7. В поле «Введите код» необходимо ввести код, полученный по SMS-уведомлению на телефон, нажимаем на «Далее»

← Двухэтапная аутентификация



Подтверждение номера

Сообщение с кодом подтверждения отправлено на номер 8 (963) 429-65-53

Введите код:

Ничего не получили? Повторите попытку

НАЗАД

Шаг 2 из 3

ДАЛЕЕ

8. В следующем окне нажимаем на «Включить»

Google Аккаунт

← Двухэтапная аутентификация



Получилось! Включить двухэтапную аутентификацию?

Вы увидели, как работает двухэтапная аутентификация. Хотите включить ее для своего аккаунта Google (testovaya.20201@gmail.com)?

Шаг 3 из 3

ВКЛЮЧИТЬ

9. Если в следующем окне вышло сообщение «Двухэтапная аутентификация включена», то все настройки проведены верно

← Двухэтапная аутентификация

Двухэтапная аутентификация включена 17 мая 2020 г.

ОТКЛЮЧИТЬ

Доступные варианты второго этапа аутентификации

Второй этап аутентификации позволяет подтвердить, что пароль ввели именно вы. Подробнее



Надоело вводить коды подтверждения?

Чтобы войти в аккаунт, просто нажмите Да, использовать уведомление от Google на телефоне.

ИСПОЛЬЗОВАТЬ УВЕДОМЛЕНИЕ



Голосовое сообщение или SMS (по умолчанию)

8 (903) 424 86 53. Нажмите Подтвердить

Коды подтверждения отправляются по голосу или SMS

Добавьте дополнительные варианты для второго этапа аутентификации

Настройте резервные варианты второго этапа аутентификации, чтобы вы могли войти в аккаунт даже если другие способы проверки личности, используемые при двухэтапной аутентификации, будут недоступны.

Резервные коды

10. Для проверки верных настроек выходим с почты и заново пробуем войти в почту, вводим пароль, нажимаем на «Далее»

Go gle

yu so

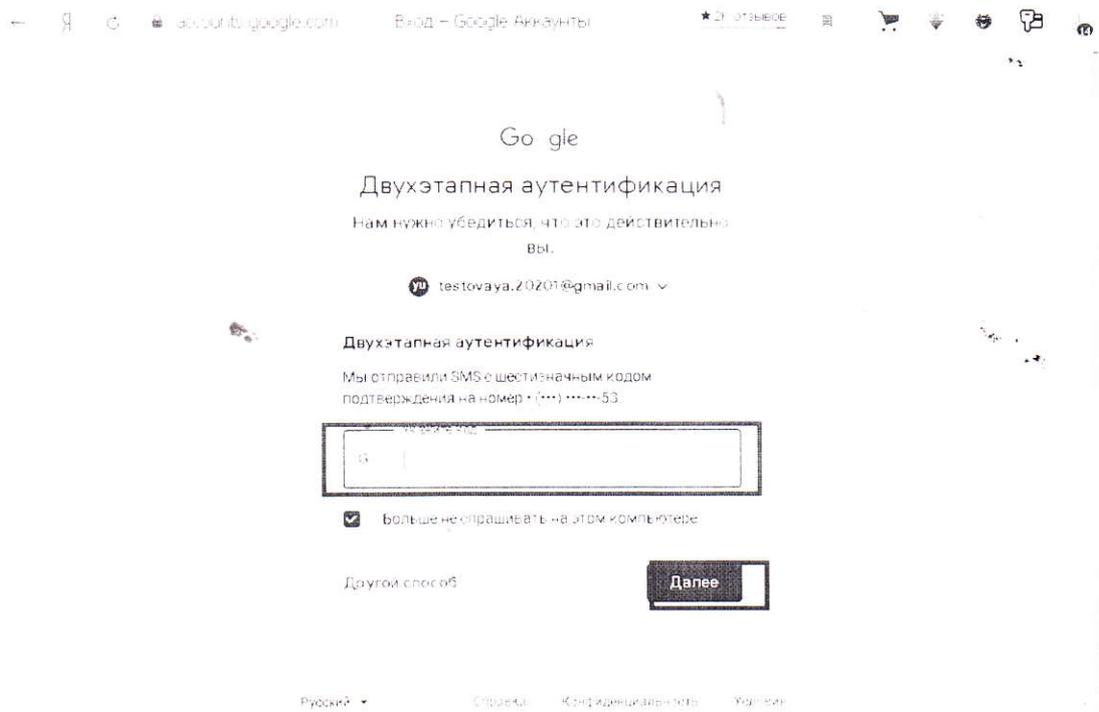
yu testovaya.20201@gmail.com

Введите пароль

Забыли пароль?

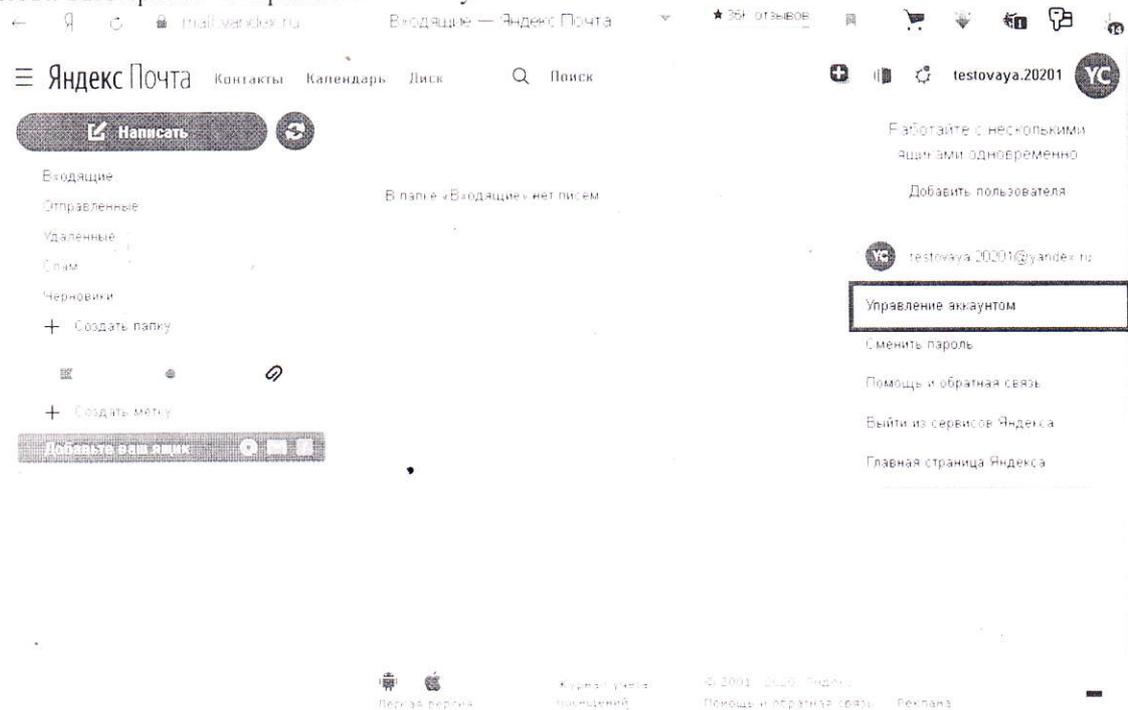
Далее

11. На телефон придет SMS-уведомление с кодом, вводим код и нажимаем на «Далее». Галочку с настроек «Запомнить на этом компьютере» при входе в почту необходимо убирать. Нажимаем на «Далее»



2.3. Настройка двухфакторной аутентификации (2FA) на почте yandex.ru

1. Слева выбираем «Управление аккаунтом»



2. Затем выбираем пункт «Настроить двухфакторную аутентификацию»

Яндекс Паспорт

testovaya.20201

Добавить фото | Указать дату рождения | Россия | Имя в комментариях и отзывах: Yu C. | Изменить персональную информацию

Пароли и авторизация

Вход без пароля

Настройка дополнительных способов входа в аккаунт

Настроить двухфакторную аутентификацию

Чтобы входить на Яндекс без пароля

Сменить пароль или контрольный вопрос

Последний раз пароль менялся минуту назад

Включить пароли приложений

Чтобы не сообщать сторонним сервисам свой пароль от Яндекса

История входов и устройств

3. Указываем номер телефона, на который будет приходить SMS-уведомление по одноразовому паролю. Формат телефона с +7 (например, +79601234567). Нажимаем на «Получить код»

Яндекс Паспорт

Управление аккаунтом | Подписки | Мои сервисы | Отзывы и оценки

Настройка двухфакторной аутентификации

Шаг 1 из 4. Укажите номер телефона

На него будет отправлен код подтверждения. Это должен быть номер на Яндекс.Паспорте. Если вы потеряете доступ к своему аккаунту

Получить код

Например: +7 xxx xxx xx xx

Вам больше не нужно беспокоиться о надежности пароля, после включения двухфакторной аутентификации вы будете заходить на Яндекс по одноразовому паролю. Его по уникальному пин-коду выдает мобильное приложение Яндекс Ключ.

Для настройки вам понадобятся два устройства: например, на планшете или компьютере вы откроете Яндекс Паспорт, а на смартфоне — Яндекс Ключ для iOS или Android.



4. Полученный в SMS-уведомлении код подтверждения вводим в поле и нажимаем на «Подтвердить»

Настройка двухфакторной аутентификации

Шаг 1 из 4. Укажите номер телефона

На него будет отправлен код подтверждения. Это ваш основной номер на Яндексе. Он понадобится, если вы потеряете доступ к своему аккаунту.

Изменить телефон

На номер +7 963 ***-**-53 отправлен код подтверждения

Код подтверждения из SMS

Подтвердить | Получить код ещё раз

Вам больше не нужно беспокоиться о надёжности пароля: после включения двухфакторной аутентификации вы будете заходить на Яндекс по одноразовому паролю. Его по уникальному пин-коду выдает мобильное приложение Яндекс.Ключ.



5. Придумываем 4-хзначный пин-код, который будет использоваться в мобильном приложении «Яндекс.Ключ». Предварительно нужно скачать приложение из Google Play Market для телефонов на Android или из AppStore для телефонов на iOS. Данное приложение будет использоваться как второй фактор при входе в почту

Настройка двухфакторной аутентификации

Шаг 2 из 4. Придумайте и запомните пин-код

Пин-код нужен каждый раз, когда вы получаете одноразовый пароль в Яндекс.Ключе, а также для восстановления доступа к аккаунту. Храните пин-код в тайне. Сотрудники службы поддержки Яндекса никогда его не спрашивают.

Введите от 4 до 10 цифр пин-кода

Пин-код: 90

Подтвердите

Создать

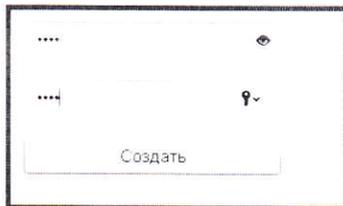
6. Затем нажимаем на «Создать»

< Настройка двухфакторной аутентификации

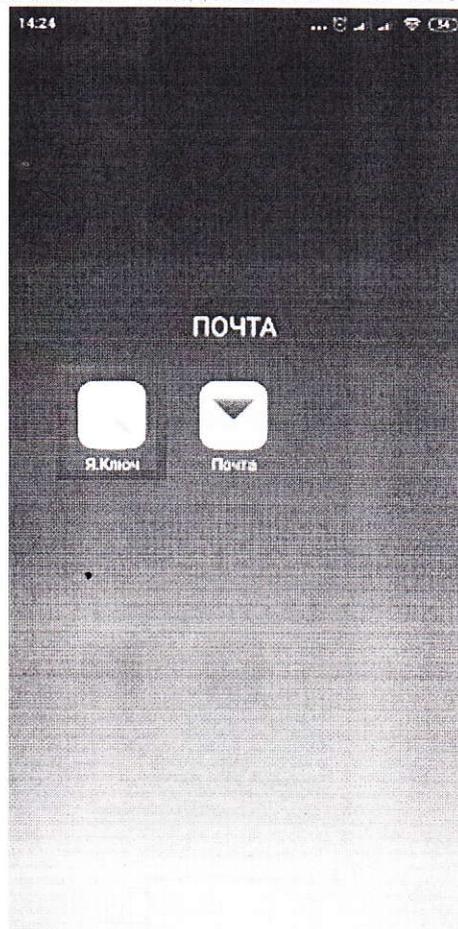
Шаг 2 из 4. Придумайте и запомните пин-код

Пин-код нужен каждый раз, когда вы получаете одноразовый пароль в Яндекс.Ключе, а также для восстановления доступа к аккаунту. Храните пинкод в тайне! Сотрудники службы поддержки Яндекса никогда его не спрашивают.

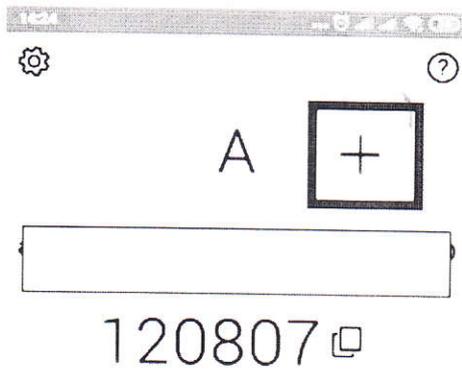
Введите от 4 до 16 цифр пин-кода



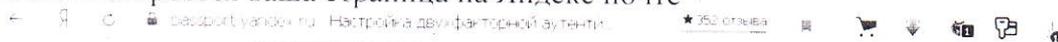
7. Запускаем мобильное приложение «Яндекс.Ключ» на телефоне



8. В окне мобильного приложения «Яндекс.Ключ» нажимаем на кнопку «+»



9. Для считывания QR-кода наводим камеру телефона на экран компьютера так, чтобы QR-код попал в рамку камеры. Чтобы убедиться в том, что все настроено правильно, нужно ввести одноразовый пароль на последнем шаге – двухфакторная аутентификация включиться, только когда вы введете корректный пароль. Если пароль введен верно, 2FA включиться и откроется ваша страница на Яндексе почте



< Настройка двухфакторной аутентификации

Шаг 3 из 4. Добавьте свой аккаунт в мобильное приложение Яндекс.Ключ

Наведите камеру телефона на QR-код, и ваш аккаунт автоматически добавится в приложение. Если считать код не удалось, попробуйте еще раз или введите секретный ключ.

Как установить Яндекс.Ключ



Покажите секретный ключ

Следующий шаг

RU

Помощь

© 2001-2020 Яндекс

10. Для проверки работоспособности двухфакторной аутентификации 2FA необходимо выйти из почты и заново в нее войти. При входе необходимо ввести логин почты. После

чего на экране появится QR-код. Для его считывания запускаем на телефоне мобильное приложение «Яндекс.Ключ», выбираем профиль почты и вводим ранее придуманный PIN-код. После чего наводим камеру телефона на экран компьютера для считывания QR-кода. После удачного считывания QR-кода автоматически будет осуществлен вход в почту.