

**О цифровой и финансовой
безопасности
жителей Чувашской Республики**

Угроза №1

Дистанционные хищения – самый актуальный тип мошенничества
более 90% от всех фактов хищения

2025 год:

30 млн попыток
телефонного мошенничества
в сутки

(2022 год - 5 млн попыток в сутки)

Угроза №1

в 2025 году

более 1 млрд рублей

жители Чувашии

отдали украинским мошенникам,

из них

около 600 млн рублей

ушло на вооружение ВСУ

и террористические удары

по России

Предлоги, с которыми мошенники обращаются к жертве

- ✓ «Попытка хищения средств или имущества», «попытка получения кредита», «продление договора сотовой связи», «переоформление кредита (в т.ч. под залог недвижимости)», «оформление сделки с объектом недвижимости», с дальнейшим переводом денег на «спец.счет», «безопасный счет» и иные счета, указанные преступниками
- ✓ «Оказание помощи полиции (прокуратуре, следственному комитету и т.п.)», «участие в спецоперации по поимке злоумышленников в банке или на объекте преступления» для «задержания работников банка или преступника с поличным»
- ✓ «Расследование по факту финансирования ВСУ» и компенсация отправленных сумм путем оформления кредитов или снятия со вкладов и направления денег на «безопасный счет»
- ✓ «Родственник «попал в беду», когда надо «срочно направить или передать деньги для «решения вопроса», для «операции» или «для проверяющих из вышестоящей организации»
- ✓ «Блокировка карты», «проблемы» с личным кабинетом на сайте Госуслуг, у оператора мобильной связи и т.п. , когда нужно подтвердить реквизиты (номера карт, пароли и коды, поступившие смс и т.п.)
- ✓ «Компенсации» («страховки», «социальные выплаты»), «перерасчет пенсии, продление услуг связи, замена домофона или счетчика, доставка цветов или товаров, голосование в интернете» и т.п. (цель мошенников - получить код доступа из СМС к госуслугам, социальным сетям или банковским приложениям жертвы)

Как они нас обманывают?

Семьи участников СВО

Переслано:
Объясняем.рф

Сегодня



Как мошенники обманывают родственников бойцов СВО?

🔔 Когда близкий человек на передовой, любая новость о нём — на вес золота. Этим и пользуются мошенники. Они придумывают истории о ранениях, наградах и выплатах, чтобы войти в доверие и украсть у людей деньги.

В специальной рубрике [Объясняем.рф](#) и [Киберполиции России](#) разбираемся, какие мошеннические схемы используют против родственников участников СВО.

🎥 Фальшивые звонки «из военкомата» или «от сослуживцев»

Мошенники связываются по телефону или в мессенджерах и представляются командирами, сослуживцами вашего близкого или волонтёрами. Часто злоумышленники владеют реальными данными и называют их для убедительности. Сценарии обмана разные:

- сообщают, что родственник получил ранение или представлен к государственной награде;
- предлагают оформить денежную выплату;
- просят денег на помощь.

Они могут попросить назвать код из СМС, перейти по ссылке, установить «нужное приложение» или перевести деньги.

Сценарий может меняться: например, фальшивые сотрудники спецслужб или военкомата могут предупреждать об «утечке данных» или запугивать уголовными делами якобы из-за финансирования недружественных стран. Под этим давлением жертву заставляют назвать код из СМС или передать наличные курьеру.

🎥 Чаты «помощи» и «поиска пропавших»

В мессенджерах мошенники создают группы и каналы для родственников, которые потеряли связь с бойцами. Цель таких чатов — не помощь, а сбор личных данных и распространение опасных файлов.

Часто эти файлы называются «список военнопленных.ark», «приложение Красного Креста.ark», «фотоальбомы пленных.ark». Устанавливать такие программы нельзя — они почти гарантированно содержат вирусы и вредоносное ПО.

🎥 Сбор данных через фото

Мошенники ищут тех, кто за деньги или под давлением согласится сфотографировать надгробия погибших участников СВО. Им нужны имена, фамилии, даты рождения и гибели — эти детали потом используют, чтобы войти в доверие к родственникам.

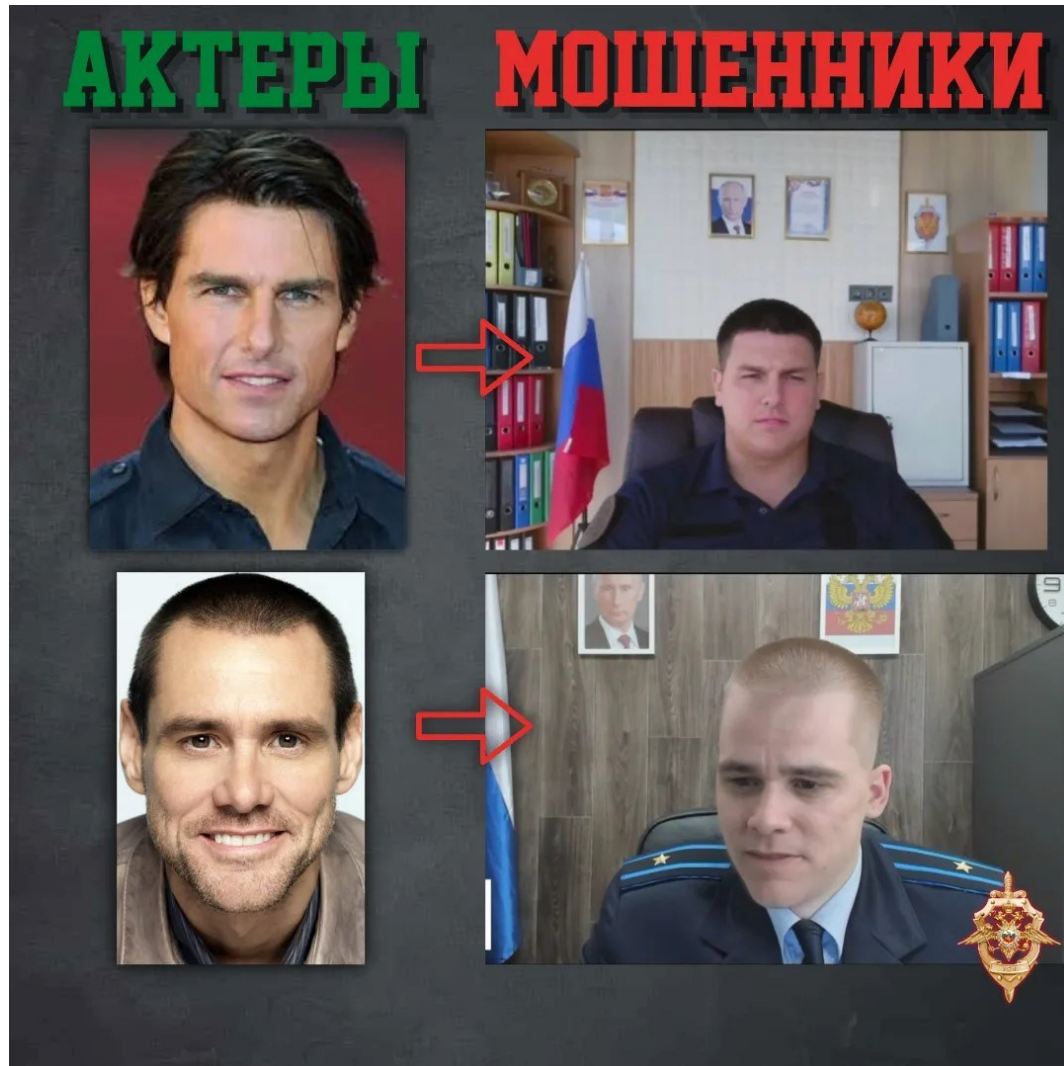
Никому не отправляйте фото захоронений и не участвуйте в сборе данных, даже если вас убеждают, что ответственности за это нет.

[@cyberpolice](#)

Технологии, которые используют мошенники

- ✓ **Оформление дубля СИМ-карты жертвы** (цель мошенников - получить коды доступа из СМС к госуслугам, социальным сетям или банковским приложениям жертвы)
- ✓ **Мошенничество в сети Интернет под видом выгодных инвестиций, в т.ч. с предложением «легкого заработка»**
- ✓ **Звонки или видеозвонки через мессенджер** (при таком звонке на аватарке виден логотип известного банка или эмблема МВД, ФСБ, Следственного комитета, Госуслуги, МФЦ или другие легко узнаваемые логотипы)
- ✓ **Звонки или сообщения от имени руководителя организации**
- ✓ **Использование нанятых курьеров для доставки фиктивных писем или повесток от «Госорганов», для получения денег от жертвы.**
- ✓ **Технология DeepFake или подмена изображения и голоса** (позволяет мошенникам создавать голосовые сообщения или видеозвонок от имени друзей и родственников, либо общаться с жертвой по видеосвязи в образе знакомого лица)
- ✓ **Мошенники могут присылать фото поддельных или нарисованных на компьютере документов и служебных удостоверений** (настоящие сотрудники правоохранительных органов, центробанка и других структур так никогда не делают!)

Примеры DeepFake – видеозвонков с изображением и голосом киноактеров (психологический эффект знакомого лица)



Как они нас обманывают?

Принципиальная схема социальной инженерии

- «Задавить авторитетом» с использованием технологии подмены номера и специфической терминологии
- Вывести жертву из душевного равновесия (страх, эйфория)
- Закрепить, подтвердить «достоверность» информации из «другого источника», в т.ч. с использованием фиктивных документов
- Нагнетание «срочности»
- Запрет на общение с другими лицами, инструктаж о «легенде»
- Длительное удержание жертвы «на телефоне»
- Управление по телефону действиями жертвы

Дополнения:

- Воздействие с отлагательным эффектом: **разделение звонков от «разных источников» по времени**
- Побуждение к совершению теракта, хулиганских, иных противоправных действий
- Имитация «похищения» человека (с хищением денег у жертвы) и **вымогательство денег** (у родственников)

Государство защищает

Какие меры введены

- ✓ Маркировка звонков
 - Запрет на получение сообщений от Госуслуг во время разговора
- ✓ Самозапрет на получение кредитов и займов
 - Запрет на действия с недвижимостью без личного участия
- ✓ Самозапрет на заключение новых договоров об оказании услуг связи (на приобретение сим-карт)
- ✓ Период охлаждения при обращении за кредитом или займом
 - Ограничения при снятии наличных в банкоматах
- ✓ Сервис «второй руки»
 - «Спецкнопка» для жалоб в банковском приложении
- ✓ Защита от мошенников в микрофинансовых организациях (МФО)

ЧТО ДЕЛАТЬ?

✓ НИЧЕГО НЕ ДЕЛАТЬ!

- ✓ НЕ сообщать кодов из СМС и вообще никаких сведений
- ✓ НЕ совершать никаких действий с деньгами и имуществом
- ✓ НЕ устанавливать никаких программ из неизвестных источников и не включать демонстрацию экрана на телефоне или ином гаджете
- ✓ НЕ переходить по интернет-ссылкам в сообщениях
- ✓ НЕ совершать противоправных действий

**Если Вы все же успели назвать код из СМС,
сообщить какие-то сведения о себе, своих счетах и т.п.:**

- Немедленно прервите общение с мошенником
- Поменяйте пароль на Госуслугах
- Срочно сообщите в банк о случившемся и инициируйте блокировку своих карт (счетов) и прекращение каких-либо сделок от Вашего имени
- Сообщите о случившемся в полицию (сохранив номер звонившего или текст переписки с мошенником)

ЧТО ДЕЛАТЬ?

Установить САМОЗАПРЕТ:

- ✓ На получение
кредита
- ✓ На сделки
с недвижимостью
без личного участия
- ✓ На активацию
сим-карты
(договора связи)

Установление запрета на получение кредита

Услуга поможет установить запрет на заключение с вами кредитных договоров

Чего не коснётся запрет

Ипотечных, образовательных
и автокредитов

Какой запрет можно установить

- Полный, который включает в себя все виды запретов
- На дистанционное и очное получение кредита в кредитной или микрофинансовой организации

Срок оказания услуги

2 календарных дня

Запрет на действия с недвижимостью без личного участия

Вы можете запретить регистрацию сделок без вашего участия или снять такой запрет

Что даст запрет

Ответьте на несколько вопросов и узнайте, что делать дальше

Начать

Профиль

Сим-карты



Запрет на оформление договоров связи

 Запрет установлен с 24.09.2025

[Подробнее](#)

Личные номера

Данные получены 24.09.2025 [Обновить](#)

Глава Подмосковья Воробьев поблагодарил тех, кто помогал семьям жертв теракта в «Крокусе»

Во вторник, 30 апреля, прошла
панихида по погибшим



ФОТО: https://t.me/vorobiev_live

Со дня теракта в «Крокус Сити
Холле» прошло 40 дней.

Правда о Telegram

За 3 последних года с помощью мессенджера совершено боле 153 000 преступлений, в т.ч. 33 000 преступлений диверсионно-террористической направленности.

Мессенджер применялся боевиками и их кураторами при организации страшного теракта в «Крокус Сити Холле» в марте 2024 года - погибли 149 человек, 609 получили ранения.

К общему количеству преступлений, совершенных с использованием Telegram, относится и массовое кибермошенничество - десятки тысяч пострадавших, ущерб от которого превысил 62,7 млрд рублей.

Обманутых все через тот же Telegram втягивали дальше в совершение диверсионно-террористических актов, в том числе в качестве «био-дронов» и «живых бомб».

Эти и многие другие преступления оказалось невозможно предотвратить в связи с отказом Telegram от взаимодействия с правоохранительными органами.

Еще мессенджер стал главной площадкой **для открытой пропаганды** суицида, буллинга, «колумбайна»**, криминальной идеологии «АУЕ»*, массовых убийств, ЛГБТ*, детской порнографии, продажи наркотиков и мошеннических схем.

*Запрещенная в России экстремистская организация.**Запрещенное в России террористическое движение.

Правда о Telegram

Правоохранители направили Telegram **более 150 тысяч запросов на удаление незаконной информации. Администрация Telegram отказалась сотрудничать, все запросы были проигнорированы, а чаты и каналы продолжают работать в следующих количествах:**

Детская порнография – 1369 чатов и каналов

Пропаганда нетрадиционных ценностей (извращений) - ЛГБТ* - 2596

Наркотики – 3771

Суицид – 2666

Азартные игры – 2134

Призывы к участию в НЕзаконных массовых мероприятиях (митингах и т.п.) – 3431

Вовлечение несовершеннолетних в иные преступления – 2124

Призывы к экстремизму - 10 598 чатов и каналов

Материалы экстремистских и террористических организаций – 7045

Финансирование терроризма – 2162

Незаконная финансовая деятельность и поддельные документы – 3898

Недостоверная финансовая информация и мошенничество - 104 093 чата и канала

*Запрещенная в России экстремистская организация.

<https://www.kp.ru/daily/27765/5213807/>

Правда о Мах



FRANK MEDIA

устройства. Мах требует те же разрешения, уточняет эксперт, что и другие приложения по типу WhatsApp*.

«Мах не запрашивает ничего нового по сравнению с другими приложениями – все работает точно по тем же правилам», — резюмирует Зураб Белый.

Пользователи в сети проверяли активность мессенджера через разные утилиты. Frank Media изучили часть обзоров, которые они выкладывали в публичный доступ. Один из авторов на Habr узнавал о работе Мах через блокировщик рекламы и трекеров AdGuard [2]. Он отслеживал те запросы, которые делал мессенджер к системе, в доступа к файлам ОС, камере другим функциям. Эксперимент



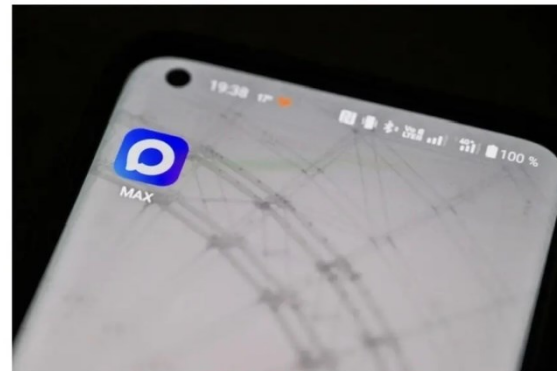
газета.ru @ Новости

26 декабря 2025, 11:16

В мессенджере Мах удалили более миллиона вредоносных файлов

Мессенджер Мах заблокировал более 700 тысяч подозрительных аккаунтов в 2025 году

Дарья Колаш



© Владимир Астапкович/РИА Новости

Мессенджер Мах заблокировал более 700 тысяч подозрительных аккаунтов в 2025 году благодаря сотрудничеству с российскими специалистами по кибербезопасности. Об этом

Вестник Киберполиции Ро...
8 929 подписчиков

Вестник Киберполиции России
Не игнорируйте автоматические уведомления

Для дополнительной защиты от мошенников мессенджер MAX запустил автоматическое уведомление о входящих звонках с неизвестных номеров. Теперь, если абонента нет в списке контактов, во время вызова отображается пометка «Нет в контактах», а при звонке из-за рубежа - наименование страны.

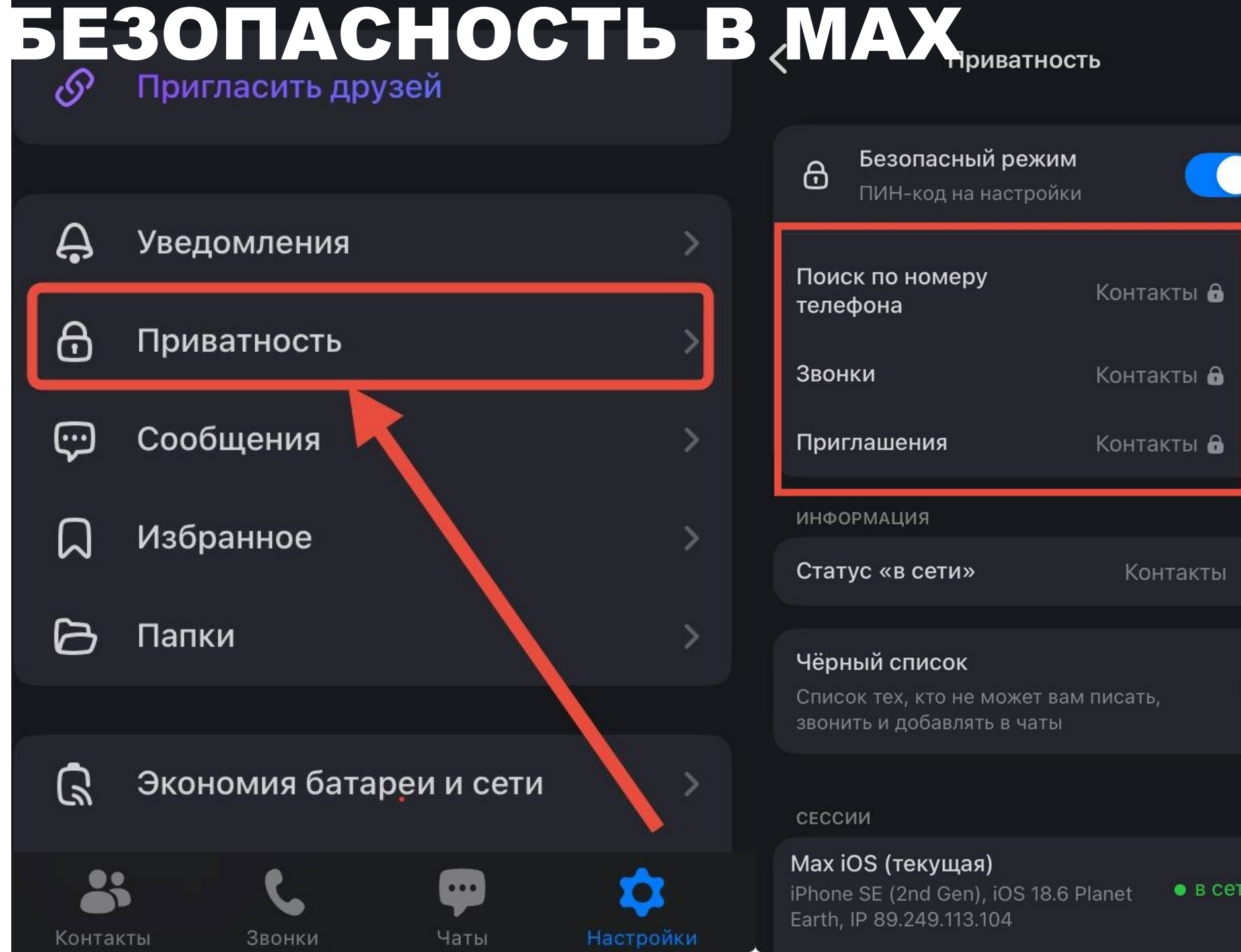
Функция начнет работать автоматически после обновления приложения.

Подписаться на Киберполицию России

61 4 2 2

17:56

БЕЗОПАСНОСТЬ В MAX



Больше полезной информации:



Наш сайт



Мы в VK



Мы в MAX