

# Как новый закон поможет защитить бизнес от мошенников: разъяснения Минцифры

С 1 июня 2025 года в России начнёт действовать закон № 41-ФЗ, направленный на борьбу с телефонными мошенниками, навязчивыми звонками и фейковыми сообщениями. Документ уже называют самым важным шагом по защите цифровых коммуникаций. Минцифры объяснило, как эти меры помогут бизнесу обезопасить клиентов, сотрудников и критически важные процессы.

## Только официальные каналы связи — никакого WhatsApp и Viber

Организациям, включая банки, операторам связи и госструктурам, запретили использовать иностранные мессенджеры для общения с клиентами. Это значит, что сообщения о «поддержке безопасности» или «предложении кредита» через WhatsApp или Telegram — верный признак мошенничества.

### Что это значит для бизнеса:

Компании смогут лучше отстроить свои официальные каналы связи. Это упростит коммуникацию с клиентами и снизит риски, когда мошенники прикрываются именем известной организации.

### Что важно сделать:

Убедитесь, что все клиенты знают, откуда им действительно может прийти сообщение. Обновите политики связи, исключив иностранные мессенджеры.

## Верификация продавцов на маркетплейсах через Госуслуги

Продавцы онлайн-площадок смогут подтверждать свою личность через Госуслуги. После этого на их профиле появится специальная отметка, которая подтверждает, что это реальный поставщик, а не фальшивка.

### Как это поможет компаниям:

Это снижает вероятность столкнуться с мошенниками при закупках товаров или услуг. Особенно это важно, если вы работаете через маркетплейсы и не можете проверить контрагента напрямую.

### Пример:

Если поставщик просит предоплату, а отметки о верификации нет — это повод насторожиться.

## Новый порядок защиты аккаунтов на Госуслугах

Теперь во время телефонного разговора Госуслуги не будут присылать коды подтверждения. Они поступят только после завершения звонка. Это убирает одну из главных уязвимостей: передачу кодов под давлением.

### Что это меняет:

Снижается риск, что сотрудник случайно передаст доступ злоумышленнику, думая, что общается с техподдержкой.

### Практический совет:

Всем, кто использует Госуслуги для работы — от оформления субсидий до проверки

юридических данных, — стоит проинструктировать сотрудников: коды по телефону не сообщаются вообще.

## **Возможность запретить оформление сим-карт на своё имя**

Через Госуслуги или МФЦ теперь можно установить самозапрет на регистрацию новых сим-карт без личного присутствия.

### **Зачем это бизнесу:**

Мошенники часто регистрируют фейковые сим-карты на ничего не подозревающих людей. Через эти номера могут проходить мошеннические звонки или регистрация на сомнительных сайтах — уже от вашего имени.

### **Что сделать:**

Руководителям компаний, владельцам бизнеса и сотрудникам с доступом к корпоративной информации стоит сразу включить самозапрет.

## **Назначение доверенных лиц для банковских операций**

Можно будет указать человека, который будет дополнительно подтверждать банковские действия. Это касается, например, переводов средств или открытия счёта.

### **Почему это важно:**

Это снизит риск несанкционированных операций. Особенно полезно для владельцев бизнеса, которые хотят обезопасить свои финансы и защитить родственников от обмана.

### **Пример:**

Компания может назначить финансового директора как доверенное лицо — и все крупные переводы пройдут только после его подтверждения.

## **Маркировка звонков и возможность отказа от спама**

При входящем звонке на экране теперь будет отображаться название организации. Кроме того, появится опция полного отказа от нежелательных звонков.

### **Преимущества для бизнеса:**

Сотрудникам проще распознавать важные и безопасные звонки: от банков, службы доставки или госорганов. Мошенники и «холодные» продавцы теряют доступ.

### **Что важно:**

Настройте маркировку на рабочих телефонах и заранее откажитесь от нежелательных вызовов. Это сэкономит время и снизит стресс сотрудников.

## **Что нужно сделать бизнесу прямо сейчас**

Закон уже принят, и большая часть положений начнёт действовать с июня 2025 года. Чтобы использовать его возможности, достаточно внедрить несколько простых шагов:

1. Переведите все коммуникации в официальные каналы.
2. Обновите инструкции по безопасности для сотрудников.
3. Установите запрет на оформление сим-карт без присутствия.
4. Настройте маркировку вызовов и откажитесь от спама.
5. Используйте верификацию поставщиков на маркетплейсах.
6. Назначьте доверенных лиц для подтверждения операций.

Закон № 41-ФЗ — это не просто защита граждан, это практический инструмент для бизнеса. Он помогает закрыть уязвимости в коммуникации, расчётах и безопасности данных.

Используйте новые правила уже сейчас, чтобы минимизировать риски и сосредоточиться на

развитии — а не на устранении последствий мошенничества.

**Читайте также** Выплата аванса сотрудникам