

ФИНРАЗУМ
15.05.2026 | 13:00

Экономический
факультет
МГУ
имени
М.В. Ломоносова



финансовая
грамотность в вузах
Федеральный сетевой методический центр



Выплаты по ОСАГО до 2 млн рублей — что будет с тарифами?

- Правительственная комиссия по законопроектной деятельности одобрила проект поправок, увеличивающий лимит выплат по ОСАГО до 2 млн руб.
- Основная причина изменений: гармонизация с выплатами в рамках ОСГОП — обязательное страхование ответственности перевозчика

	Ущерб имуществу	Ущерб жизни и здоровью
Сейчас	400 тыс. руб.	500 тыс. руб.
Будет	400 тыс. руб.	2 млн руб.

Выплаты по ОСАГО в 2025 году	Сумма выплат, руб.	Число выплат
Ущерб жизни	1,8 млрд	4,7 тыс.
Ущерб здоровью	2,6 млрд	21,4 тыс.
Ущерб имуществу	158,7 млрд	1,5 млн

Добровольное страхование самозанятых

- Первые результаты пилотного проекта по добровольному социальному страхованию (налог на профессиональных доход не дает права на больничный и пенсию)
- Из **16 млн** страховку купило **20 тыс.** человек (эксперимент с 1 января 2026 по 31 декабря 2028 года — 456-ФЗ от 15.12.2025).
Но нет другой работы у 25% самозанятых
- **Условия — 3.84% вноса от суммы выплаты**
 - взносы 1344 руб. в месяц — страховое покрытие 35 тыс. руб.
 - взносы 1920 руб. в месяц — страховое покрытие 50 тыс. руб.
 - только больничный — все 100% после 8 лет стажа (до этого меньше). Декретных и детских выплат нет.



«Народные облигации» — это...

«Народные облигации» — это специальные долговые ценные бумаги, которые предназначены исключительно для покупки обычными гражданами. В отличие от обычных облигаций, **они не торгуются на бирже**, часто имеют фиксированный доход и продаются напрямую эмитентом через банки или платформу Финуслуги.

- Низкий вход — купить можно на небольшую сумму.
- Нет биржи — они не торгуются на рынке, поэтому нет рискованных скачков цены.
- Досрочный выкуп — обычно вы можете потребовать вернуть деньги раньше срока, не теряя проценты.
- Простой и понятный **инструмент для новичков**.

Обычно их выпускает государство или регионы (на развитие дорог, инфраструктуры).

Но есть и корпоративные «народные» облигации — и **история «Евротранса» — как раз такой случай.**



Что случилось с Евротрансом?

«Евротранс» (сеть АЗС «Трасса») **перестал выкупать свои народные облигации**. Деньги тысяч инвесторов **заблокировались**. Напомним, что продать на рынке нельзя, а только эмитенту!

- Инвесторы (без вины виноватые) не могут вернуть вложения — компания не платит с апреля.
- Акции упали до «**исторического дна**» (71,5 руб., а раньше стоили 140+ руб.).
- Обычные облигации торгуются по 34–60% от номинала — это признак больших проблем.

Начинающие инвесторы пострадали,
а есть выход? Только ждать, если Евротранс выкупит облигации....
А если нет?



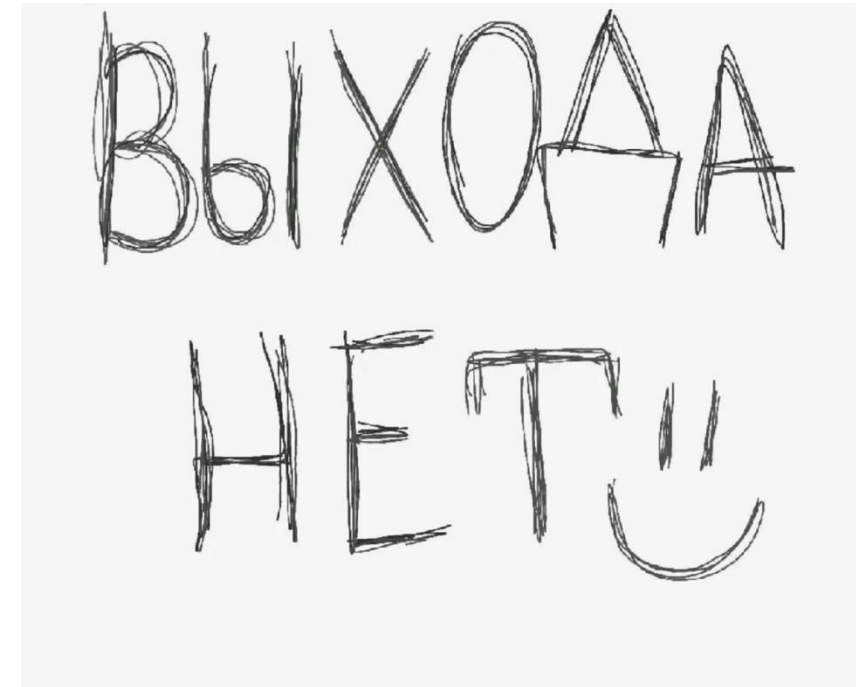
Как компания «Евротранс» впала в транс...

«Евротранс» годами платил высокие дивиденды... в долг, к сожалению, у компании отрицательный денежный поток.

В отчете за 2025 год:

- Свободный денежный поток (FCF) — минус 19,8 млрд руб.
- Чистый долг вырос до 37 млрд руб.
- А Капитализация компании — всего 13 млрд руб. (значит, долг уже не погасить).
- За 3 года выплатили ≈ 70 руб. дивидендов на акцию.

«Выхода нет» — компания перестала публиковать информацию для инвесторов.

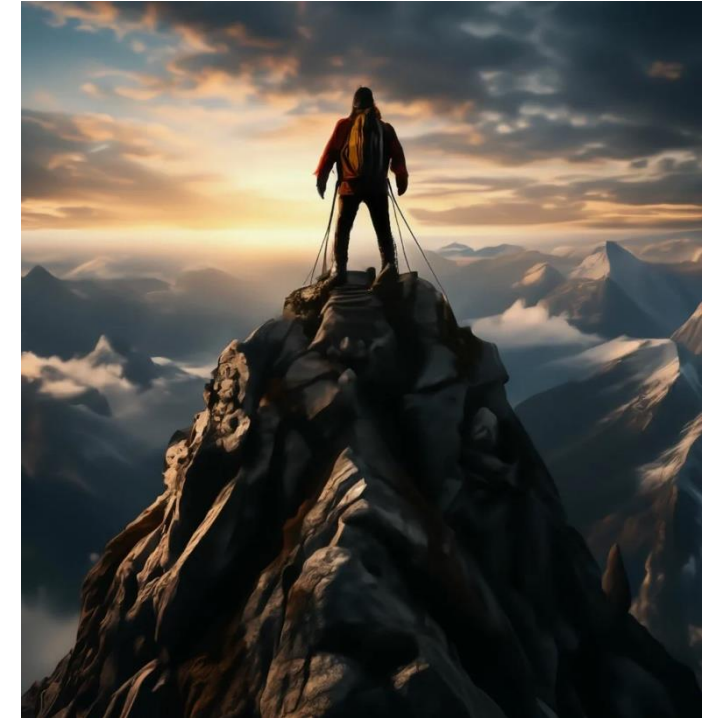


Риск потерять есть всегда!

«Народные» облигации НЕ дают полной защиты, если вдруг у эмитента возникли финансовые проблемы.

- Инвесторы в отсутствии возможности продать на вторичном рынке оказались в ловушке, поскольку эмитент отказывается выкупать бумаги.
- Высокая дивидендная доходность (у «Евротранса» она была 22%) может «неожиданным сюрпризом». Оценивать компанию нужно, в том числе с учетом денежного потока и долга.

К сожалению, по оценке экспертов, целевая цена акций «Евротранса» — 0 руб. (вероятность банкротства может быть достаточно высокой).



<https://shdevrum.ai/post/4be8b2af9bed11eea510ae4273cd71f1?share=e48pgh5jreg1uhty2g0rzhtm0g>

«Ковровый» СМС-бомбинг и «добрый спасатель»

Ловушка — злодеи массово вводят номер телефона жертвы на сайтах интернет-магазинов, аптек, банков, МФИ и прочих сервисов услуг. На пострадавшего приходит шквал СМС-сообщений с кодами подтверждения. До нескольких сотен сообщений — это безжалостный СМС-бомбинг!

В попытке разобраться, а что происходит?

Наносится 2 удар: поступает звонок от подставного сотрудника «службы банка» или «сотового оператора.»

Мошенник убедительно заявляет, что прямо сейчас злоумышленники пытаются взломать аккаунты пользователя, — это «атака хакеров»!

В панике, человек диктует коды из СМС, чтобы остановить атаку.



Как защитить себя и не пострадать?

Если **приходит лавина СМС** с кодами — не паникуйте. Отключите звук, не отвечайте на сообщения и не переходите по ссылкам.

1. Паника — это инструмент мошенников!

2. Никому и никогда не диктуйте коды из СМС. Ни сотрудник банка, ни полицейский, ни оператор связи никогда не попросят вас назвать код подтверждения.

3. Не переводите деньги на «безопасные счета». Это миф — таких счетов нет!

4. При СМС-бомбинге можно **временнo включить авиарежим** или заблокировать все входящие сообщения через настройки телефона.

5. **Свяжитесь с вашим оператором сотовой связи и банком** сообщите о случившемся. Оператор сможет временно ограничить поток рекламных и сервисных СМС на ваш номер. Звонок в банк по надежному номеру для проверки.



Шокирующее видео — Вы нарушитель!

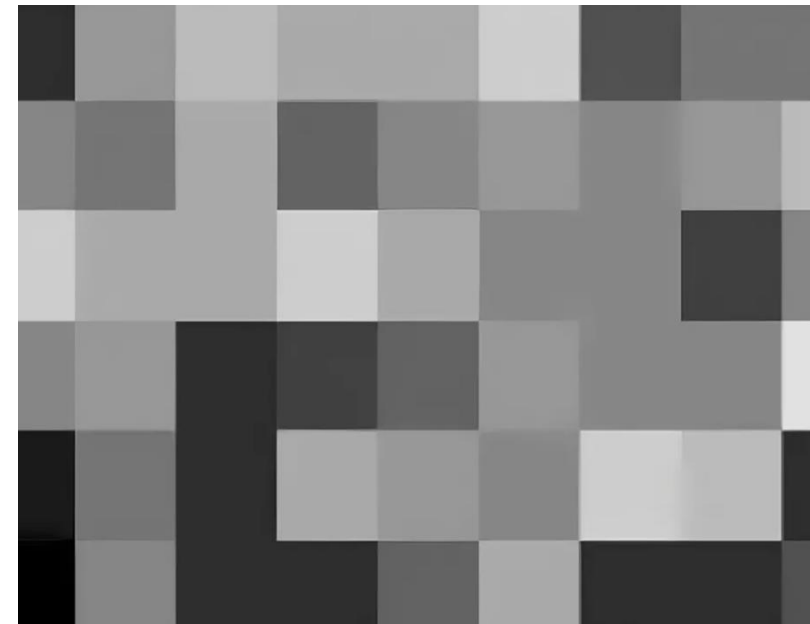
1 удар — по психике. Мошенники создают фейковую страницу «Госавтоинспекции» и сообщают пользователю, что тот якобы совершил нарушение во время вождения. Видео с камеры — с номером машины, датой и местом.

«А вдруг я действительно кого-то задел? А вдруг придет штраф или лишат прав?» **Страх — мы готовы на все, чтобы «прояснить ситуацию».**

2 удар — через чужую трагедию. На другом сайте злоумышленники публикуют анонсы «эксклюзивных видео со страшными автоавариями». Злодеи указывают выдуманные подробности: дату, время, количество погибших и раненых.

Смесь ужаса и болезненного любопытства — «как это было»?

1 клик — «специальное приложение для просмотра», вредоносное ПО — кража паролей.



Как защитить себя и не пострадать?

1 правило: смотреть видео только на официальных ресурсах. Настоящая Госавтоинспекция не рассылает ссылки на скачивание приложений для просмотра нарушений. Проверь адрес сайта через поисковик и не переходим по ссылкам из сообщений или рекламы.

2 правило: никогда не качайте «специальные приложения для просмотра видео». Если сайт предлагает установить программу, чтобы открыть ролик — это почти наверняка вирус. Настоящие видео открываются в браузере или стандартном плеере.

3 правило: используйте антивирусное программное обеспечение. Хороший антивирус блокирует фишинговые сайты и предупредит перед скачиванием подозрительного файла.

Любое обещание шокирующего или запретного контента скорее всего нелегально.



<https://shedevrum.ai/post/0169a464725311eeb033badf81d486ab/>

Цифровой щит — обман на доверии!

Мошенниками был создан фишинговый ресурс, замаскированный под просветительский портал по кибергигиене — «Цифровой щит».

«**Тест**» пароля уязвимость вымышленным «российским стандартам криптостойкости 2026 года».

Для этого человека **просят ввести пароль от реального сервиса.**

Приманка к теме собственной безопасности, создавая иллюзию защищенности, а в действительности инициируют утечку конфиденциальных данных.

Создать надежную «цифровую броню»! Многие пользователи повторяют 1 пароль на нескольких ресурсах, добытая таким образом строка позволяет злодеям **взломать десяток аккаунтов.**



Как защитить себя и не пострадать?

Никогда не вводите свои реальные пароли на непроверенных сайтах. Сервис никогда не попросит прислать ваш пароль в открытом виде «для проверки».

Длинные пароли не нужно нигде «проверять» — они сами по себе надежны. Пароль вроде «ПОМНЮ ЧУДНОЕ МГНОВЕНИЕ» содержит более 30 символов, включая пробелы и разные регистры.

Для перебора такой пароль потребует сотни лет — проверять его «устойчивость» не нужно и опасно.

Придумайте личную ассоциацию и сделайте ее немного нелепой — это не забывается!

Альтернатива — использовать генераторы случайных паролей. Программы-менеджеры паролей создают уникальные сложные пароли.

Регулярно **меняйте пароли, но без фанатизма:** (почта, банки, госуслуги) не реже раз в 2–3 месяца.



Осторожно, дети!

Достаточно 15 секунд из голосовых сообщений и с помощью ИИ создают почти 100% копию голоса (голосовой дипфейк).

Вашему ребенку от лжеродителя от знакомого. Идет команда — дать код из СМС, заставить перейти по ссылке, перевести деньги либо просто втянуть в разговор, чтобы снизить бдительность.

Дети — удобная мишень! Они живут в цифровой мире, активно общаются в мессенджерах, доверяют голосу и легко поддаются на контакт, который выглядит привычным и безопасным.

В 6 раз выросло количество случаев с использованием цифровой копии голоса. **Мерзкий обман: слышу родной голос — значит, можно верить.** Но сегодня голос уже не является доказательством личности.



Как защитить себя и не пострадать?

Главное — доверительный диалог с ребенком. Ребенок должен знать, что в любой тревожной ситуации он может сразу **обратиться к взрослым и не бояться наказания.**

2 Правило — Личное кодовое слово в семье. Например: «**Саймон сказал...**» Любую важную просьбу или информацию от родственника ребенок проверяет через кодовое слово. Не назвали слово — не верь.

Тренировка в игре «Мошенник и жертва».

Родитель и ребенок меняются ролями: один пытается обмануть, другой — распознать угрозу. Это формирует навык без запугивания.

Ребенок — Шерлок Хомс по кибербезопасности!

Дайте ребенку задание регулярно узнавать о новых схемах мошенников и информировать всю семью.



<https://shedevrum.ai/en/post/b0d28cf9750811ee9c29b646b2a0ffc1?share=e48pgh5jregl1uhty2g0rzhtm0g>

ВОПРОСЫ



Марат Шамилевич **Сафиулин**
Сергей Анатольевич **Трухачев**
Валентина Сергеевна **Трушина**

ФИНРАЗУМ
29.05.2026 | 13:00

Экономический
факультет
МГУ
имени
М.В. Ломоносова



финансовая
грамотность в вузах
Федеральный сетевой методический центр

«КАК РАЗГОВАРИВАТЬ СО СТУДЕНТАМИ О НЕДВИЖИМОСТИ II»

