

# 谁在“收割”投资者焦虑

## ——起底自媒体荐股乱象

# 国家继续对成品油价格采取调控措施

新华社北京4月7日电(记者魏弘毅 魏玉坤)记者7日从国家发展改革委了解到,3月23日国内成品油价格调整以来,国际市场原油价格大幅震荡。为减缓国际油价上涨对国内的冲击,国家继续对成品油价格采取调控措施。

按照成品油价格机制计算,自4月7日24时起,国内汽油、柴油(标准品)价格每吨应分别上调800元、770元,调控后实际上调420元、400元。

# 减缓国际油价上涨冲击

## ——解读本次汽油、柴油价格调控

新华社北京4月7日电(记者魏玉坤 魏弘毅)国家发展改革委7日发布消息,按照成品油价格机制计算,自4月7日24时起,国内汽、柴油价格每吨应分别上调800元、770元,调控后实际上调420元、400元。

专家表示,3月23日国内成品油价格调整以来,国际市场原油价格大幅震荡。为减缓国际油价上涨对国内的冲击,国家继续对成品油价格采取调控措施。

国家发展改革委价格成本和认证中心副处长吕指巨表示,本次汽、柴油最高零售价格每桶上调800元、400元,少涨380元、370元,折合92号汽油每升少涨0.31元,0号柴油每升少涨0.32元。初步测算,私家车加满一箱油可少支出15元左右;大货车加满一箱油可少支出150元至200元。



荐股陷阱 新华社发 商海春 作

境实施的“荐股引流+虚假投资”类电信网络诈骗案件。犯罪集团成员分工配合,以投资黄金“高收益”为诱饵,通过伪装资深投资者、打造明星导师、制造盈利假象等方式,层层诱导被害人落入陷阱,造成巨额财产损失。

中山大学国际金融学院教授陈增祥表示,一些财经“大V”往往喜欢吹嘘成、暴富,鼓励短线投机与追涨杀跌,扭曲了健康的投资文化。大量散户在“大V”建议下采取同质化交易策略,可能在特定时点加剧市场波动。

### 揭秘“股神”套路

从名不见经传的普通博主,到万人追捧的“荐股大师”,一些自媒体从业者并非拥有过人的投资经验,而是掌握成熟的“造神”套路:

——打造“人设”,铺设“掘金”起点。

一部分自媒体人精心包装权威形象,顶着“投资顾问”“理财师”等光鲜头衔吸引粉丝。

一名在短视频平台拥有23万粉丝的财经“大V”,其认证头衔为某公司理财师。但经查,该公司实际属于科技推广和应用服务业,并非持牌金融机构。

一些“指点金融市场”,发布“投资建议”的财经“大V”,甚至不具备相关资质。

当前,各大平台上的金融类账号认证要求认证者持有相关资质证书,但一些没有任何资质的从业者,通过花钱也能买“认证”。有运营人员表示,某短视频平台“拿下资质证书+帮认证”仅需2500元,另一社交服务平台认证财经博主则要5500元。

——编造虚假投资战绩,塑造可信度。

鲜为人知的是,股市上“所谓”每天百万的收益,只需一个“股票模拟器”便可达成。在网购平台上,25元便可购买一个仿真的股票模拟器。一名售卖模拟器的商家告诉记者,模拟器与真实交易的实盘界面相似,但后台盈亏数据可以随意修改。

此外,那些看似精准的“超前预测”,更是简单的障眼法。

一些财经博主在开盘前同时发布“看多”和“看空”的帖子并隐藏,收盘后公开正确的一版,便营造出“百猜百中”的假象。

——私域引流变现,将投资者带入“灰色地带”。

更值得注意的是,一些不良自媒体从

业者一旦积累了足够人气,便通过添加个人微信、组建投资社群等方式,将粉丝引导至监管难以触及的私域地带。

记者调查发现,财经博主在公共平台大多会用“仅供参考,不构成投资建议”等话术进行形式上的合规包装,但一旦投资者添加了投资助理的微信,便会抛开违规荐股的“遮羞布”——助理会明确表示,付费即可获得精准的股票代码和买卖点建议。

陈增祥指出,这些财经博主多采用多平台分发、矩阵化运营模式。引流、付费、服务环节相互分离,主账号与小号、“马甲”号联动运作。一旦被监管警示或封禁,可快速切换平台继续运营。

### 多方协同“查漏补缺”

受访专家指出,整治自媒体荐股乱象,亟需监管部门、相关平台形成合力,从制度完善、源头管控等多方面入手,查漏补缺、标本兼治,共同规范行业发展,保护投资者合法权益。

2025年,中央网信办发布关于规范网络名人账号行为管理的通知,将未经许可或未取得相应资质擅自从事荐股投资等行为纳入负面清单,为常态化监管提供了依据。

陈增祥表示,监管部门还需进一步明晰法律定性与监管边界,明确财经知识付费与持牌投资咨询、证券期货经营活动的区分标准,防止以知识分享为名开展非法

金融业务。

网络平台需从源头端切实履行主体责任,加强全流程管理。

陈增祥建议,平台应从源头强化资质审核,对明显缺乏专业背景的博主、存在违规问题的内容,及时采取限制传播、下架处置等措施。同时,要规范营销宣传行为,严禁算法助推焦虑式营销、煽动性内容,建立对伪造交易记录、夸大收益等违规情形的快速识别与拦截机制。

今年以来,已有平台陆续采取行动。雪球一日之内封禁22个财经“大V”,重点整治非法证券投资咨询及违规引流行为;知识星球也发布公告,深度清查“非法经济学家”及无资质违规课程。严禁售卖未经合规备案、含有非法荐股、分成跟投等违法违规内容的课程或产品。

对投资者而言,树立理性投资观念、提升风险识别能力,是保护自身财产安全的最重要防线。陈增祥说,合规的投资指导,其核心特征是,由持牌金融机构及其从业人员在法定业务范围内开展,以投资者教育和适当性服务为目的,而非直接售卖“致富秘籍”“内幕消息”。

北京市鑫诺律师事务所律师董高升提醒,投资者需摒弃“低风险高收益”“快速致富”等不切实际的预期,认清资本市场的风险本质。若投资者遭遇侵权行为,应注重证据留存,及时向平台投诉反馈,或向监管部门、公安机关举报违规线索,维护自身合法权益。

# 非法收受财物数额特别巨大

## 检察机关依法对叶寒冰涉嫌受贿案提起公诉

新华社北京4月7日电 记者4月7日从最高人民检察院获悉,四川省政府原党组成员、副省长,省公安厅原党委书记、厅长叶寒冰涉嫌受贿一案,由国家监察委员会调查终结,移送检察机关审查起诉。最高人民检察院依法以涉嫌受贿罪对叶寒冰作出逮捕决定,并指定由重庆市人民检察院第五分院审查起诉。近日,重庆市人民检察院第五分院已向重庆市第五中级人民法院提起公诉。

检察机关在审查起诉阶段,依法告知了被告人叶寒冰享有的诉讼权利,并讯问了被告人,听取了辩护人的意见。检察机关起诉指控:被告人叶寒冰利用担任浙江省公安厅治安总队总队长,浙江省温州市委常委、市公安局局长,浙江省公安厅副厅长,杭州市委常委、市公安局局长,四川省副省长、省公安厅厅长等职务上的便利,以及职权或者地位形成的便利条件,为他人谋取利益,非法收受他人财物,数额特别巨大,依法应当以受贿罪追究其刑事责任。

# 清明假期全国口岸日均出入境人员226万人次

## 边检机关及时疏导客流高峰

新华社北京4月7日电(记者孙鹏程)记者4月7日从国家移民管理局获悉,今年清明假期全国边检机关共保障677.9万人次出入境,日均226万人次,较去年同期增长9.1%;单日出入境通关最高峰出现在4月6日,达233.4万人次。

国家移民局介绍,清明假期期间,港澳台居民出入境329.1万人次,较去年同期增长19.5%;外国人出入境84.3万人次,较去年同期增长20.9%。入境外国人中,适用免签政策入境31.9万人次,较去年同期增长30.7%。此外,共计查验出入境交通运输工具30.7万架(艘、列、辆)次,较去年同期增长13.3%。

据了解,全国边检机关按照国家移民局统一部署,科学预测、及时发布本口岸出入境客流情况,提示广大出入境人员合理安排行程;科学组织勤务,配足执勤警力,针对港澳台居民、海外华人华侨返乡祭祖人数多、老年人多等实际情况,设置专门查验通道,为需要特殊照顾旅客提供帮助;密切部门协作联动,及时疏导客流高峰,确保口岸通关高效顺畅。清明假期,全国口岸出入境安全便捷、井然有序。

# 国开行落实一次性信用修复政策惠及13.3万名国家助学贷款借款人

据新华社北京4月7日电(记者张千千)记者4月7日从国家开发银行获悉,国家开发银行认真落实《中国人民银行关于实施一次性信用修复政策有关安排的通知》要求,截至今年3月底,共帮助13.3万名国家助学贷款借款人享受到一次性信用修复政策。

去年12月,中国人民银行对外发布一次性信用修复政策有关安排。据介绍,针对由国开行承办的国家助学贷款,若逾期发生在2020年1月1日至2025年12月31日期间,单笔合同累计逾期本息不超过1万元,且借款人在今年3月31日(含)前已足额偿还逾期本息,可获得一次性信用修复。

为扎实做好相关工作,国开行通过多渠道发布相关公告,明确相关政策条件、时间窗口等,并主动向符合条件借款人发送提示短信,着力提高政策知晓率。同时,推动分行与各级学生资助管理部门密切配合,高效做好政策宣介、逾期本息回收等工作。在借款人满足一次性信用修复条件后,国开行第一时间更新报送征信数据,帮助他们尽早享受政策红利。

# 我国人工智能安全标准体系加速构建

## AI安全事件频发



2025年11月6日,观众在2025年世界互联网大会“互联网之光”博览会现场参观。新华社记者 黄宗摄

新华社北京4月7日电《经济参考报》4月7日刊发记者叶健、吴蔚采写的文章《AI安全焦点追踪|我国人工智能安全标准体系加速构建》。文章称,随着我国“人工智能+”行动的深入推进,各类智能体及AI应用广泛渗透生产生活场景。而近期频发的AI安全事件,不仅引发公众关注,也成为产业界与学界协同攻坚的重要方向。近日,全国网络安全标准化技术委员会(以下简称“网安标委”)正式组建“人工智能安全标准工作组”(WG9),标志着我国人工智能安全标准体系建设进入系统性推进阶段。

### AI安全事件频发 攻防之战升级

近期,全球人工智能行业安全事件频发。3月底,人工智能公司Anthropic旗下AI编程工具Claude Code源代码泄露,这一事件被视为AI行业首次核心代码泄露事件。

奇安信安全专家章磊认为,综合各类公开信息以及Anthropic的官方回应分析,此次源代码泄露是典型的发布流程中

的人为失误,属于供应链安全事故。“好比原本只该给顾客成品,结果把全套制作图纸一起送出去了。”

“产品的核心逻辑和防护底线一旦公开,整个产品的运作方式就变得透明。竞争对手可以直接研究它的架构、功能设计、智能体逻辑,能快速模仿、追赶甚至优化。同时,安全规则暴露后,也更容易被人找到漏洞、绕过约束、破解使用限制。”章磊表示。

今年以来爆火的智能体工具Open-Claw(俗称“龙虾”)也接连曝出存在多重安全隐患。4月3日,国家信息安全漏洞库(CNNVD)发布通报称,自3月10日至4月2日,共采集OpenClaw漏洞155个,其中超危漏洞11个、高危漏洞53个,OpenClaw多个版本受到漏洞影响。

“我们只花了一个下午,就攻破了OpenClaw。”国内知名白帽安全团队DARKNAVY安全创新总监陆晨表示,目前,国内主流的“龙虾”方案分为两类:一类是在OpenClaw基础上套壳提供对话框,另一类是提供服务器供用户自行配置。相比较而言,前者风险更高,一旦被攻破,黑客就能直接获取服务器权限,甚至访问内网大模型。

上海交通大学安泰经济与管理学院副院长刘少轩透露,近期一家制造业企业因为仓促上马OpenClaw,导致产线停产72小时,直接损失可能超过2000万元。还有一家法律服务企业,因为没有做好风险防范和数据安全,导致大量客户隐私数据泄露。

亚信安全相关负责人也指出,当前网络攻击正在向智能化、自动化演进,黑客利用AI实现勒索软件载荷的动态生成、高仿真钓鱼内容制作,使得攻击效率与隐蔽性大幅提升。AI自主攻击智能体、基于深度伪造的商务诈骗,将成为2026年最紧迫的安全挑战。

### AI安全供给发力 需求创造机遇

国资委1月底发布的数据显示,中央企业已在工业制造、能源电力、智能网联汽车等重点领域,打造了超过1000个AI应用场景,AI赋能产业转型的态势日益明显。与此同时,AI安全问题引发的行业担忧,也催生了全新的安全需求,推动AI安全供给持续发力。

对此,东莞证券认为,近期OpenClaw等智能体技术快速落地,催生全新安全需求场景,叠加网络安全领域政策利好持续释放,行业有望迎来新的增长机遇。

长江证券则预测,2026年国内网络安全市场规模有望突破1500亿元,2030年可达3000亿元,年复合增长率达18%至20%,行业正处于发展黄金期。

同时,AI安全新品与服务也在持续发布。近日,上海人工智能实验室推出高安全产业级智能体平台SafeClaw,聚焦高安全需求的产业智能化转型,以推动行业从“事后安全”迈向“内生安全”的路径。同时,上海人工智能实验室还开源了能快速诊断风险的智能体守卫模型,并探索将安全准则内嵌至智能体决策层的“内生进化”治理框架。

“最危险的并非已知风险,而是‘没有想到的危险’,因此,当前的核心任务是,在AI能力飙升的同时,前瞻性地构建内生安全体系。”上海人工智能实验室领军科学家胡侠表示,“这些工作旨在将安全能力深度融合AI发展全链条,为智能体时代的‘内生安全’提供系统性解决方案。”

至访问内网大模型。

上海交通大学安泰经济与管理学院副院长刘少轩透露,近期一家制造业企业因为仓促上马OpenClaw,导致产线停产72小时,直接损失可能超过2000万元。还有一家法律服务企业,因为没有做好风险防范和数据安全,导致大量客户隐私数据泄露。

### AI治理持续完善 安全标准加速制定

随着人工智能被广泛应用,人工智能治理也越发受到重视。今年政府工作报告明确提出“完善人工智能治理”,全国人大常委会工作报告提出“加强人工智能领域立法研究”。

在此背景下,人工智能安全标准正在加快制定。3月25日,工信部公开征求《人工智能安全治理模型》上下文协议应用安全要求》等行业标准计划项目意见。

4月初,人工智能安全标准工作组(WG9)表示,将重点推动《网络安全技术 人工智能安全能力成熟度评估方法》《网络安全技术 人工智能应用安全分类分级方法》及《网络安全技术 人工智能技术涉及未成年人应用安全指南》等核心标准的落地实施。同时,在全国网安标委统一部署下,集中力量攻坚内生安全与数据基座、新形态与服务安全、系统与应用安全及科学评测等领域的国家标准。

“针对AI带来的新型风险,需从政策法规、技术标准、实施机制三个层面协同推进。”奇安信副总裁张勇认为,展望未来,安全将从“可选配”升级为“必标配”,安全合规将从推荐性转向强制性,可以设定“AI安全投入不低于AI应用总投入15%”这样的行业基准;第二,网络安全从“单点防护”走向“全链条协同”,实现“一处发现攻击,全网自动免疫”;第三,从“人防”走向“技防+智防”,AI对抗AI成为攻防常态;第四,从“被动应急”走向“主动免疫”,构建韧性防御体系,实现“即使遭受攻击也能快速恢复、核心数据不丢失”。