UDC 343.98:343.35
DOI: 10.63341/naia-herald/2.2026.20

ISSN 2410-3594
E-ISSN 2786-7382

Strategies for counteracting obstruction of pre-trial investigations into criminal offences in the context of official duties

Oleksandr Amelin*
PhD in Law, Associate Professor
Office of the Prosecutor General
01011, 13/15 Riznytska Str., Kyiv, Ukraine
Educational and Scientific Institute of Law of State Tax University
08201, 31 Universytetska Str., Irpin, Ukraine
https://orcid.org/0000-0002-0933-2111

■ **Abstract.** The study aimed to identify strategies for countering obstruction and to develop a system of tactical approaches to protect pre-trial investigations into official misconduct from disruptive influences. The research was based on a combination of comparative legal analysis, quantitative analysis of official statistical data, and qualitative analysis of judicial and investigative practice. Based on a comparative legal analysis of legislation and case law in Ukraine, the United States of America and the Federal Republic of Germany, a systematisation of tools for neutralising and overcoming resistance from specific actors was conducted. The study established that, in contrast to retrospective countermeasures, the strategy of threat neutralisation involves the pre-emptive freezing of a suspect's administrative and financial resources before irreversible consequences arise. The analysis of empirical data has confirmed the effectiveness of a three-tiered response system to counter-investigation activities, which involves a combination of financial, technological and procedural measures. The study determined that the priority approach is to deprive the official of economic benefit, as evidenced by the practice of asset freezing in foreign jurisdictions and the use of settlement agreements. The effectiveness of using mass decryption of encrypted messaging apps and blockchain analysis to identify hidden links in high-tech schemes involving cryptocurrency mixers has been demonstrated. This research demonstrated the need to implement international standards of accountability for interference with the administration of justice and to expand the powers of anti-corruption bodies to intercept information autonomously from telecommunications networks to minimise leaks. The practical value of the study is determined by the potential for direct application of the proposed recommendations to improve criminal procedure legislation

■ **Keywords**: influence; pressure; threats; overcoming; evidence; seizure of assets; plea agreements; search; investigative measures; offences in the course of duty; corruption; case law

■ Introduction

The research relevance is determined by the radical transformation of the mechanisms used to obstruct the investigation of criminal offences in the sphere of official duties, which, in the context of martial law and European integration processes, has taken on the characteristics of a high-tech, coordinated and well-resourced operation. Modern official crime, exploiting legislative loopholes and administrative influence, has shifted the focus from the primitive destruction of evidence to the creation of complex intellectual obstacles, requiring pre-trial investigation bodies to change their response paradigm: from

■ **Suggested Citation:**
Amelin, O. (2026). Strategies for counteracting obstruction of pre-trial investigations into criminal offences in the context of official duties. *Scientific Journal of the National Academy of Internal Affairs,* 31(2), 20-36. doi: 10.63341/naia-herald/2.2026.20.

■ *Corresponding author (*yuamelinoleksandr@gmail.com*)

■ Received: 02.02.2026; Revised: 01.05.2026; Accepted: 26.05.2026; Published: 01.06.2026

reactively overcoming the consequences to proactively neutralising threats.

The extent to which this issue has been explored in academic research is reflected in the considerable interest shown by scholars in specific aspects of countermeasures. The fundamental underpinnings of crimes committed in the course of senior-level official duties, and the specific means employed by specialised actors to evade accountability, were examined by M.L. Benson *et al.* (2024). The study demonstrated that high-ranking actors exploit institutional loopholes as "windows of opportunity" to commit and conceal crimes and revealed the symbiotic links between state and corporate crime, which require specific control methods. P. Gottschalk (2024) analysed the institutional barriers and challenges faced by national anti-corruption bodies in various countries, identifying patterns of organisational resistance at the level of state structures and illustrated the dilemmas faced by governments when auditing such bodies.

An analysis of the nature and structure of the mechanism for obstructing investigations was conducted by O. Tarkan (2025), identifying the structural elements of this activity and the stages of its implementation in the context of a criminal conflict. The study argued that the mechanism of obstruction is a dynamic phenomenon involving preparation, active interference with evidence and the concealment of traces, which necessitates the integration of the forensic characteristics of obstruction into investigative methodology. The specifics of administrative investigations and the phenomenon of using bureaucratic procedures as a "psychological weapon" against regulatory bodies were studied by A.A. Gavoor & S.A. Platt (2022). Using specific case studies, the researchers demonstrated how protracted and non-transparent investigations can be used to exert pressure on businesses, which is key to determination of the limits of the authorities' powers. The psychological aspects of the behaviour of those involved, in particular the self-justification techniques (guilt neutralisation) used by fraudsters during interrogations, were the subject of a study by K. Majid & A. Kapure (2025). Their findings identified key defence strategies employed by suspects, such as denying harm or shifting blame, and proposed methods for countering them during investigative proceedings.

A separate section of studies was devoted to tactical techniques and procedural measures aimed at obtaining evidence in conflict situations. For instance, O.Yu. Amelin (2025a) analysed the body search as a tool for gathering evidence in criminal proceedings concerning unlawful gain. The study demonstrated the synonymy of the terms "personal search" and "body search" and justified the need to simplify the procedure for conducting such searches under martial law to improve efficiency. The issues of tactical support for the investigation of corruption offences and the role of preventive measures were examined by M.O. Kassimova *et al.* (2023). The researchers analysed the concept of investigative prevention in the post-Soviet space and concluded that current legislative regulation is often insufficient for the full realisation of this potential. The authors emphasised that eliminating formalism in approaches to crime prevention is a key factor in enhancing the effectiveness of the fight against corruption.

The issue of ensuring the safety of participants in criminal proceedings and preventing interference with them was examined by O. Krykunov *et al.* (2023). Their study justified the expediency of granting operational units the right to immediately monitor individuals identified during searches, with a view to the early prevention of threats to witnesses. Meanwhile, V. Cherniei *et al.* (2022) highlighted criminal law and institutional instruments, highlighting certain inconsistencies between Ukrainian state policy and international standards governing the interaction between the authorities and the public. The researchers emphasised that the system of measures to combat corruption must be based on the principles of publicity, transparency and the inevitability of punishment. The limits of procedural influence were demonstrated by H. Boreiko & V. Navrotska (2023) in a comparative analysis of the abuse of the right to prosecute in Ukraine and the USA. The study determined that the improper use of discretionary powers by a prosecutor undermines the interests of justice in both jurisdictions. This necessitates the development of legitimate measures to counter procedural obstruction to safeguard the rights of parties to the proceedings.

Despite a substantial body of academic research, the sources analysed did not clearly distinguish between the concepts of "overcoming" (as a reactive action) and "neutralisation" (as a proactive action), specifically in the context of service-related offences. Most authors treated these processes as synonymous or in a fragmented manner, emphasising individual investigative actions whilst neglecting a comprehensive strategy that combines procedural, tactical and administrative measures. Furthermore, the issue of adapting international experience to the realities of martial law in Ukraine remained insufficiently researched.

The study aimed to identify strategies for countering resistance and to develop a set of techniques for mitigating threats to the investigation of official crimes. To achieve this aim, the following tasks were set: to establish the substantive differences between the concepts of "overcoming" and "neutralisation"; to conduct a comparative analysis of the effectiveness of countermeasures in Ukraine, the USA and Germany; and to develop practical recommendations

for ensuring the technical and institutional autonomy of investigative bodies.

Materials and Methods

The methodological framework of the study was based on a comprehensive interdisciplinary approach, incorporating dogmatic, comparative legal and empirical methods. The geographical scope of the study covered the legal systems of Ukraine, the United States of America (USA) and the Federal Republic of Germany (FRG). The choice of these jurisdictions was dictated by the need to compare Ukrainian practice, which is developing under the conditions of martial law, with the experience of countries that have well-established institutions for combating official corruption. The US legal system was chosen as the benchmark model for the application of plea bargain agreements and liability for obstruction of justice. Meanwhile, the experience of the FRG is relevant due to its membership of the Romano-Germanic legal family and the existence of progressive practices for neutralising cyber threats. In particular, the study compares German algorithms for the preventive "freezing" of data and methods for overcoming obfuscation of digital traces to neutralise the remote deletion of evidence even before searches commence.

The research process was structured in four stages. In the first stage, a method of semantic and legal analysis was applied to fundamental works in the field of criminal procedure, in particular, the monographic study by M.S. Tsutskiridze (2020). The choice of this source is due to its status as a foundational theoretical work, in which the nature of criminal procedural activity in conditions of conflict was conceptualised for the first time at a systemic level, and tactical foundations for neutralising opposition were proposed. This method was used to distinguish the substantive content of the categories of "overcoming" and "neutralisation" based on the temporal vector of investigative influence, namely retrospective (elimination of the consequences of the counteraction committed) or proactive (prevention of potential threats). Given the absence of direct definitions in legislation, their functional equivalents were analysed: in Ukraine, procedural mechanisms for the collection and securing of evidence (Chapters 17, 21) of the Criminal Procedure Code of Ukraine[1] concerning the seizure of property and covert investigative (search) actions; in the USA, the concept of obstruction of justice[2]; in Germany – provisions of the German Criminal Code[3] (§ 258, 258a StGB). To determine the legal limits on the application of procedural coercive measures and to define the scope of the investigator's powers, a formal-legal method was employed, which was used for an analysis of the relevant provisions of the Criminal Code of Ukraine (CC)[4] and the Criminal Procedural Code of Ukraine (CPC)[5].

In the second stage, statistical analysis was applied to data from the Office of the Attorney General (n.d.) for the period 2022-2025, to verify trends in official corruption and analyse the use of pre-trial detention as a preventive measure in the context of neutralising the influence of those implicated. Reports from the National Anti-Corruption Bureau of Ukraine (NABU) (2024; 2025) were also examined to identify the most common forms of obstruction, in particular, information leaks and the blocking of access to data. The identification process was conducted by searching the texts for semantic markers ("interference", "pressure", "data destruction", "discrediting").

The third stage was based on a case study approach aimed at examining the tactics employed by the parties in specific criminal proceedings. Analysis of materials from high-profile cases in Ukraine: The case of former Minister of Ecology Mykola Zlochevsky[6], The case of the Krayan plant[7], Case No. 521/17260/18[8], Case No. 991/1692/24[9], The case of former Supreme Court Chairman Vsevolod Knyazev[10], the "Ukrzaliznytsia" case (National Anti-Corruption Bureau of Ukraine, 2025), was conducted to verify the effectiveness of tactical approaches such as simulation of the crime scene, procedural isolation and financial neutralisation. The study of US case law in the cases of United States v. Samuel Bankman-Fried[11] and Operator of "Bitcoin Fog" (2024) was conducted to examine mechanisms for neutralising pressure on witnesses and legalising evidence from the digital

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2] U.S. Code: Title 18 – Crimes and Criminal Procedure. (1948, June). Retrieved from https://www.law.cornell.edu/uscode/text/18.
[3] German Criminal Code. (1998, November). Retrieved from https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.
[4] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[5] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[6] The case of former Minister of Ecology Mykola Zlochevsky. (2022, May). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52020000000000473.
[7] The case of the Krayan plant. (2021, March). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52016000000000411.
[8] Case No. 521/17260/18. (2019, July). Retrieved from https://clarity-project.info/court/decision/82973002.
[9] Case No. 991/1692/24. (2025, November). Retrieved from https://reyestr.court.gov.ua/Review/131931145.
[10] The case of former Supreme Court Chairman Vsevolod Knyazev. (2024, March). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52023000000000202.
[11] United States v. Samuel Bankman-Fried, a/k/a "SBF," 22 Cr. 673 (LAK). (2024, March). Retrieved from https://www.justice.gov/usao-sdny/united-states-v-samuel-bankman-fried-aka-sbf-22-cr-673-lak.

reconstruction of transactions. At the same time, an analysis of German court decisions in the cases of EncroChat[1], Wirecard (Bushuev, 2022) and Tandler (Ott, 2023) were conducted to substantiate the admissibility of evidence.

The fourth stage used the comparative law method to identify ways of improving national legislation. Analysis of US legislation: U.S. Code: Title 18 – Crimes and Criminal Procedure[2]; Foreign Corrupt Practices Act of 1977[3]; 9-47.120 – FCPA Corporate Enforcement Policy[4] and West Germany: The German Criminal Code[5] and the German Code of Criminal Procedure[6] were examined to identify the most appropriate wording for provisions concerning liability for obstruction of justice. A study of European directives: Directive (EU) No. 2019/1937 of the European Parliament and of the Council "On the Protection of Persons Who Report Breaches of Union Law"[7], the Act for the Better Protection of Whistleblowers[8] The recommendations of the United Nations Office on Drugs and Crime (2025) were conducted to develop algorithms for the protection of whistleblowers. A limitation of the study is the use exclusively of open data from court registers and official reports from law enforcement agencies.

Results

A doctrinal distinction between the concepts of "overcoming" and "neutralisation". The effectiveness of pre-trial investigations into criminal offences in the sphere of official duties is directly linked to the prosecution's ability to identify, anticipate and counteract the evasive tactics employed by the perpetrators. In legal doctrine and law enforcement practice, the terms "overcoming" and "neutralisation" are used to describe the response of authorised persons to the destructive influence of suspects, and these terms are often mistakenly equated. However, a semantic and logical-legal analysis, conducted through the prism of the specific nature of "white-collar" crime, has revealed a significant substantive difference between these concepts (Table 1).

Table 1. A comparative analysis of the tactical and legal nature of the concepts of "overcoming" and "neutralising" obstruction of an investigation

Comparison criteria	Overcoming	Neutralisation
Direction of action	Retrospective (a reaction to the past)	Proactive/preventive (a pre-emptive action)
Tactic description	Breaking through an established barrier, overcoming active resistance	Neutralising the opposing force, rendering the threat harmless before any consequences arise
Nature of the countermeasures	Physical destruction of evidence, falsification of documents, refusal to testify	Misuse of administrative resources, digital obfuscation, and preparation for data destruction
Form of conflict	Open confrontation (search met with resistance, interrogation)	Covert/hidden struggle (NS(R)D, account freezing)
Key tools	Forensic investigations (data recovery), further questioning, and temporary access	Suspension from office, freezing of assets, infiltration by undercover agents, and digitisation of the process in the form of "iCase"
The psychological effect	Overcoming the suspect's resistance	Creating conditions under which resistance becomes technically or legally impossible

Source: compiled by the author based on the German Criminal Code[9], U.S. Code: Title 18 – Crimes and Criminal Procedure[10], Criminal Procedural Code of Ukraine[11], M.S. Tsutskiridze (2020)

[1] CaseC-670/22, M.N. (EncroChat): Judgment of the Court (Grand Chamber) (request for a preliminary ruling from the Landgericht Berlin – Germany) – Criminal proceedings against M.N. (Reference for a preliminary ruling – Judicial cooperation in criminal matters – Directive 2014/41/EU – European Investigation Order (EIO) in criminal matters – Obtaining of evidence already in the possession of the competent authorities of the executing State – Conditions for issuing an EIO – Encrypted telecommunications service – EncroChat – Need for the decision of a judge – Use of evidence obtained in breach of EU law). (2024, April). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62022CA0670.

[2] U.S. Code: Title 18 – Crimes and Criminal Procedure. (1948, June). Retrieved from https://www.law.cornell.edu/uscode/text/18.

[3] Foreign Corrupt Practices Act of 1977. (1977, December). Retrieved from https://www.govinfo.gov/content/pkg/COMPS-9569/pdf/COMPS-9569.pdf.

[4] 9-47.120 – FCPA Corporate Enforcement Policy. (2019, March). Retrieved from https://www.justice.gov/criminal/criminal-fraud/file/838416/dl.

[5] German Criminal Code. (1998, November). Retrieved from https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

[6] German Code of Criminal Procedure. (1987, April). Retrieved from https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html.

[7] Directive (EU) No. 2019/1937 of the European Parliament and of the Council "On the Protection of Persons Who Report Breaches of Union Law". (2019, October). Retrieved from https://eur-lex.europa.eu/eli/dir/2019/1937/oj/eng.

[8] Act for the Better Protection of Whistleblowers. (2023, May). Retrieved from https://www.gesetze-im-internet.de/englisch_hinschg/englisch_hinschg.html.

[9] German Criminal Code. (1998, November). Retrieved from https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

[10] U.S. Code: Title 18 – Crimes and Criminal Procedure. (1948, June). Retrieved from https://www.law.cornell.edu/uscode/text/18.

[11] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.

As noted by M.S. Tsutskiridze (2020), an investigator's criminal procedural activities in a context of conflict require a determination of the nature of the obstacles that arise during the presentation of evidence. The application of the semantic method has established that the term "overcoming" is etymologically linked to passing through an existing obstacle or achieving victory overactive resistance. From a criminalistic perspective, overcoming activities are predominantly retrospective in nature, as the investigator is compelled to react to an act of obstruction that has already taken place. The legal basis for classifying such actions is provided by the Criminal Code of Ukraine.[1], in particular Article 358 (Forgery of documents, seals, stamps and forms) and Article 366 (Official forgery). A specific example of such a situation in proceedings concerning the misappropriation of budget funds (Article 191 of the Criminal Code of Ukraine) is the case of embezzlement within the structure of "Ukroboronprom", where officials of the state-owned enterprise paid 146 million UAH for fictitious "agency services" relating to the sale of military equipment. In this case, the source documentation was falsified: contracts and service provision certificates were drawn up in the names of foreign front companies, although in reality, all the efforts were made by the state-owned enterprise's staff. In this case, the investigator's strategy aims to recover lost information by obtaining temporary access to items and documents, and commissioning forensic economic and handwriting analyses, which essentially constitutes a process of "overcoming" an already established barrier24. Economic expert reports and the analysis of financial flows established that the "agency agreements" had no real substance, and that the transferred funds were subsequently distributed among the members of the criminal group. Another example of retrospective counteraction is the giving of false testimony by subordinate employees under pressure from management. In cases of official misconduct, the heads of an institution may exploit the administrative dependence of staff by threatening dismissal or disciplinary action. A specific example of such tactics is an organised group uncovered in the Odesa region, which operated directly within the judicial system to organise schemes for the illegal departure of conscripts abroad. Under this scheme, court decisions were issued on fabricated grounds, granting a father sole custody of a child, thereby creating fictitious legal grounds for crossing the border. The internal hierarchy and the involvement of staff disguised the unlawful activities as legitimate judicial proceedings. According to analytical reports by the National Anti-Corruption Bureau of Ukraine, individuals under investigation (senior officials and heads of state-owned enterprises) use corporate resources and messaging apps (Signal, WhatsApp) to brief witnesses and coordinate defence strategies even before the first summons for questioning (National Anti-Corruption Bureau of Ukraine, 2024; 2025). In such a situation, the investigator faces an already established obstacle, which must be overcome by conducting simultaneous interrogations and using data obtained as a result of covert investigative (search) operations (C(S)O). To verify the intensity of resistance and assess the effectiveness of measures to counter it, statistical indicators were analysed (Table 2).

Table 2. Statistics on persons who have committed criminal offences in the course of their official duties (2022-2025)

	2022	**2023**	**2024**	**2025**
Total number of persons informed of suspicion	85.285	108.271	108.387	93.139
Total number of individuals informed of suspicion of crime in the sphere of official duties	4.808	5.916	7.570	7.394
% of the total number of persons informed of suspicion	5.6%	4.8%	7%	8%
The number of individuals who have committed offences in the course of their duties and in respect of whom a special pre-trial investigation has been conducted	3	7	13	3
The number of persons who committed offences in the course of their duties and in respect of whom criminal proceedings were closed on exonerating grounds	2	5	1	0
The number of persons who committed offences in the course of their official duties and in respect of whom criminal proceedings have been discontinued pursuant to paragraph 10 of Part 1 of Article 284 of the Code of Criminal Procedure of Ukraine	0	0	0	0
The number of persons subject to pre-trial detention as a preventive measure for committing offences in the course of their duties	43	62	78	121

Source: compiled by the author based on Office of the Attorney General (n.d.)

An analysis of the data in Table 2 confirmed a shift in the focus of investigations towards proactive prevention. Firstly, despite general fluctuations in the number of suspects, the segment of white-collar crime showed steady growth – from 4,808 individuals in 2022 to 7,394 in 2025 (an increase of 53.8%).

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.

Secondly, the most significant development is the almost threefold increase in the number of cases where pre-trial detention was applied (from 43 to 121 individuals). This trend is a direct tactical response to attempts by suspects to use their status to exert pressure: the investigation is increasingly opting for the complete isolation of the suspect as a means of neutralising their influence. Thirdly, the zero figure for cases closed on rehabilitative grounds in 2025 demonstrates that the use of stringent neutralisation measures (such as pre-trial detention) is accompanied by an improvement in the quality of the evidence base. Even with a decrease in the number of special investigations (*in absentia*), this indicates not a decline in activity, but a more effective neutralisation of the risk of flight at the initial stage. This approach correlates with the high effectiveness of anti-corruption bodies, in particular the National Anti-Corruption Bureau of Ukraine (2025), during the reporting period of 2025, the economic impact of whose activities exceeded UAH 16.8 billion, representing the amount of restitution for high-level corruption offences.

In contrast, the category of "neutralisation" has a broader tactical scope, particularly concerning individuals vested with authority. Semantically, this term refers to counterbalancing opposing forces or rendering a threat harmless before irreversible consequences arise. In the case of official crimes, where perpetrators possess administrative resources and knowledge of investigative methods, neutralisation – which encompasses preventive measures – is the priority. The implemented strategy for the digital transformation of criminal justice has shifted the main focus of countering resistance to the cyber domain, where the priority task has become ensuring the integrity of electronic data sets and pre-emptively halting high-tech attempts to compromise investigative operations. It involves preventive blocking of access to electronic evidence (cloud storage, servers, corporate email) until such time as it is remotely destroyed by the suspects (Puddister & McNabb, 2021; Stepaniuk, 2025). Neutralisation is aimed at blocking the very possibility of using one's official position to obstruct the investigation. A classic procedural tool for neutralisation is the suspension of an official from office in accordance with Article 154 of the Criminal Procedure Code of Ukraine[1]. This measure severs the administrative link between the suspect manager and potential subordinate witnesses, depriving the subject of the countermeasure of their means of influence. An analysis of how the courts apply these categories in the context of actual resistance confirms the validity of proactive tactics. A three-tier model for overcoming resistance was applied in the case of the former head of the Supreme Court. At the first stage, the defendant's multi-layered defence system, which included the use of a "back office" and secure communication channels, was neutralised by a combination of undercover infiltration (cooperation with a notary acting as an intermediary) and technical surveillance, which made it possible to record the receipt of 2.7 million USD directly in the defendant's office. In the second stage, the chosen tactics were legally validated in court. Attempts by the defence to discredit the evidence through claims of "provocation of a crime" were rejected by the Appeals Chamber of the High Anti-Corruption Court (HACC), which effectively recognised the agent's active conduct within the closed environment of the criminal group as a permissible means of documentation[2,3]. The final institutional neutralisation in this case was achieved through administrative proceedings for property-related offences, the judge's dismissal from office, and the conclusion of a plea agreement with an accomplice, which broke the chain of mutual support and finally deprived the defendant of administrative resources.

Another example is Case No. 991/1297/22[4]. In Ukrainian judicial practice, this case has become a model of how to comprehensively counter multi-layered resistance; an analysis of it has made it possible to trace the evolution of the parties' tactics from active resistance to procedural compromise. At the initial stage, an attempt to bribe the leadership of the anti-corruption authorities with a record bribe of 6 million USD was neutralised by the prosecution using tactics to simulate the circumstances of the crime, which made it possible to document the chain of intermediaries and apprehend them in the act. Subsequently, during the trial phase, the defence resorted to legal sabotage, securing the return of the indictment on the grounds of an allegedly forged prosecutor's signature (ruling of the High Anti-Corruption Court of 19 October 2022[5], however, this form of legal obstruction was swiftly neutralised by judicial review, when the Appeals Chamber of the HACC overturned the unfounded ruling and resumed proceedings. The final act of the confrontation was a plea bargain, used to counter the tactics of evading

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2] The case of former Supreme Court Chairman Vsevolod Knyazev. (2024, March). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52023000000000202.
[3] Case No. 991/1692/24. (2025, November). Retrieved from https://reyestr.court.gov.ua/Review/131931145.
[4] The case of former Minister of Ecology Mykola Zlochevsky. (2022, May). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52020000000000473.
[5] Ibidem, 2022.

justice while the defendant was abroad. The investigation utilised proceedings *in absentia*, followed by a reclassification of the charges, which culminated in the approval of a plea agreement and the financial neutralisation of the consequences of the offence in the form of voluntary compensation for defence costs amounting to over UAH 660 million. In this case, the allocation of funds intended for corruption to defence needs during wartime was deemed a higher tactical priority than the protracted effort to overcome procedural obstruction by the defence.

The experience of the United States of America and the Federal Republic of Germany has shown that the effective neutralisation of obstruction is based on legislative provisions establishing liability for the very act of obstruction, even in the absence of serious consequences. Thus, in the US legal system, the offence of Obstruction of Justice, codified in the US Code: Title 18 – Crimes and Criminal Procedure[1], serves as a tool for neutralisation. In particular, Section 1512 provides for liability for "Tampering with a witness, victim, or an informant". The American model of tactics is based on the presumption that any attempt to exert pressure on participants in the proceedings constitutes a separate serious offence. This neutralises obstruction in the US by initiating parallel criminal proceedings for the act of obstruction, even before the investigation into the main official offence has been completed. Such tactics create a "self-neutralising" effect. In other words, the risk of receiving a lengthy prison sentence for pressuring a witness may outweigh the benefit of concealing the main offence. In Germany (FRG), Section 258 of the German Criminal Code[2] establishes liability for obstruction of justice (Strafvereitelung). German doctrine on the investigation of official offences (Amtsdelikte) emphasises the tactic of "sudden freezing of assets and data". According to German practice, neutralising obstruction is achieved through synchronised searches (Durchsuchung) of offices and private premises, which prevents accomplices from coordinating their actions (European Union Agency for Criminal Justice Cooperation, 2024). Crucially, German legislation clearly distinguishes between the passive right to defence and active obstruction of the investigation. In particular, the German Criminal Code criminalises actions aimed at creating fabricated evidence and manipulating information, classifying them under paragraph 258 (Obstruction of Justice), as well as 267 (Falsification of Documents) and 269 (Falsification of Evidence). This approach makes it possible for German law enforcement agencies to hold officials accountable not only for the main corruption offence, but also separately for each attempt to falsify digital or paper-based information carriers.

An analysis of law enforcement practice, as reflected in the National Anti-Corruption Bureau of Ukraine's Report (2025) for the first half of 2025, indicates that the effectiveness of investigations depends on the speed of response to information leaks and the use of the latest digital tools, in particular the "iCase" electronic criminal proceedings system, software tools for monitoring unauthorised access to state registers, and tools for conducting complex cross-border financial investigations. As noted in the report, one of the most dangerous forms of counteraction has been the use by suspects of insider information to conceal evidence even before the active phase of implementation begins. The report's empirical data highlights the scale of such information-based countermeasures: investigators uncovered a scheme involving unauthorised monitoring of the restricted section of the Unified State Register of Court Decisions, through which the perpetrators conducted 39,615 search queries and viewed 7,572 rulings by investigating judges. Access to this data made it possible for the defence to stay one step ahead of law enforcement, warning clients of planned searches and seizures of property, which created conditions for the destruction of material evidence and the concealment of assets. In this regard, it is appropriate to view neutralisation as a comprehensive two-tier system. The first level – procedural neutralisation – involves the use of non-discretionary measures to secure criminal proceedings to prevent losses. A notable example of the effectiveness of such tactics is the case concerning land fraud at the Ministry of Community, Territorial and Infrastructure Development, where, thanks to the timely seizure of the plot, it was possible to prevent (neutralise) losses to the state amounting to 1 billion UAH as early as the pre-trial investigation stage. The second level – tactical and forensic neutralisation – is based on technological superiority and the element of surprise. In circumstances where physical document flow is vulnerable to destruction, the digitisation of the process becomes a strategic tool for neutralisation. The implementation of the "iCase" electronic criminal proceedings system, in which over 1,800 cases have already been registered, minimises the risks of physical loss of materials and ensures that traces of the crime are recorded in a digital environment inaccessible to manipulation by the corrupt networks of those involved. Furthermore, tactical neutralisation is effectively used to expose shadow management structures ("back offices"), as was the case in the "Ukrzaliznytsia" case, where NABU identified and neutralised a parallel structure that,

[1] U.S. Code: Title 18 – Crimes and Criminal Procedure. (1948, June). Retrieved from https://www.law.cornell.edu/uscode/text/18.
[2] German Criminal Code. (1998, November). Retrieved from https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

for a certain percentage, ensured victory in tenders for companies under its control. Another key aspect in distinguishing between the concepts under consideration is the psychological component of the tactics. Whilst "overcoming" involves open conflict (for example, during searches where instances of physical resistance and pressure on detectives are recorded), "neutralisation" is conducted covertly. An example is remote monitoring and analysis of digital data, which renders suspects' attempts to destroy paper "slush fund" records meaningless. Thus, the transition from reactive "overcoming" to proactive "neutralisation", underpinned by an economic benefit of UAH 16.8 billion, is the only viable direction for the development of methods for investigating official crimes.

A strategy for countering institutional and external obstruction of investigations into corruption offences. Whilst at the tactical level, obstruction of investigations involves the destruction of evidence or the influencing of witnesses, at the strategic level it takes the form of institutional resistance, which poses a far greater threat to the criminal justice system. A systematic analysis of the empirical data contained in the reports of the National Anti-Corruption Bureau of Ukraine (2024; 2025) for 2024-2025 has revealed that holders of public authority are increasingly resorting to mechanisms of external interference to deprive pre-trial investigation bodies of their functional capacity. In such circumstances, the tactics of neutralisation extend outside the criminal process and become part of a comprehensive strategy to safeguard institutional independence. Empirical evidence of the effectiveness of mobilising civil society as a tool for neutralising institutional threats is provided by a precedent documented in the Report of the National Anti-Corruption Bureau of Ukraine for the first half of 2025. During this period, anti-corruption bodies faced legislative pressure for the first time when the legislature adopted a regulatory act (Official statement of NABU…, 2025) that effectively restricted the administrative autonomy of NABU and the SAPO, and this decision was taken without discussion and contrary to the consolidated position of civil society and international partners (Patrikeeva, 2025). However, as noted in the report, the immediate reaction of the public, which sparked a significant "public outcry", proved to be the decisive factor in tactically neutralising this threat. The result of this coordinated response from the civil sector was that the legislature was subsequently forced to pass a new law, which, de jure and de facto, restored the independence of anti-corruption institutions (National Anti-Corruption Bureau of Ukraine, 2025). This case demonstrated that, in conditions of political instability, it is precisely publicity and the support of external stakeholders that act as a safeguard against attempts to dismantle the anti-corruption infrastructure. This confirmed the thesis that, in cases involving high-level official misconduct, neutralising political interference is a necessary prerequisite for initiating legal proceedings. Judicial practice confirms the possibility of neutralising "regional judicial protectionism" through mechanisms of judicial review. In the proceedings concerning the Mayor of Odesa (the "Krayan" factory case and the land acquisition scheme)[1], the systematic obstruction, manifested in the acquittal of the defendants by the court of first instance, was neutralised by the Appeals Chamber of the HACC, which overturned the questionable verdict. The new phase of curbing the use of administrative resources in 2025 was characterised by a combination of procedural measures (raising the bail amount to UAH 42 million) and extraordinary administrative measures, including the revocation of citizenship. This steps *de jure* removed the individual from positions of authority, definitively eliminating the risks of their using their office to put pressure on witnesses and obstruct the investigation.

A distinct and dangerous form of opposition identified in 2025 was the direct physical and procedural pressure exerted on law enforcement officers (National Anti-Corruption Bureau of Ukraine, 2025). The report documents instances of searches being conducted on NABU staff without the requisite court orders, as well as the use of physical force and unlawful surveillance against them. Such actions aim to psychologically destabilise personnel and intimidate investigators. The strategy for countering this involves the strict application of the legal safeguards provided for in the relevant legislation. The key instrument is the procedural recording of each instance of pressure as a separate criminal offence (interference in the activities of a law enforcement officer) and the provision of personal security for staff by special units. A significant problem that complicates investigations and creates conditions for information leaks is the technical dependence of anti-corruption bodies. According to the Report of the National Anti-Corruption Bureau of Ukraine (2024) for the first half of 2024, NABU still lacks the legal authority to autonomously obtain information from telecommunications networks, forcing it to rely on the resources of the Security Service of Ukraine. Such dependence creates risks of compromising covert investigative (surveillance) operations even at the planning stage. At this stage, a tactical approach to mitigating this vulnerability involves using alternative methods to obtain digital evidence (for example, accessing correspondence via seized physical devices rather than through traffic interception);

[1] The case of the Krayan plant. (2021, March). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52016000000000411.

however, a strategic solution to the problem is only possible through legislative changes aimed at breaking the monopoly on "wiretapping". Furthermore, the lack of an independent expert body forces NABU investigators to turn to institutions subordinate to other agencies, which also creates risks of delays in conducting expert examinations as a form of procedural obstruction. A key element of the tactic to neutralise organised opposition, which is often characterised by a code of silence ("omerta") within state institutions, is the development of the institution of whistleblowers. This approach is also being implemented in Ukraine: according to a report by the National Anti-Corruption Bureau of Ukraine (2025), based on an audit by the United Nations Office on Drugs and Crime (UNODC) (2025), new anonymity protocols are being introduced to minimise risks to whistle-blowers. In this context, the experience of Germany is instructive, where in July 2023, the Act for the Better Protection of Whistleblowers[1] was enacted, implementing Directive (EU) No. 2019/1937 of the European Parliament and of the Council[2]. The German model of neutralisation is based on the mandatory establishment of secure internal reporting channels in all organisations with more than 50 employees. This can be used by law enforcement agencies to obtain evidence against corporate executives or government officials directly from within the system, thereby undermining corporate solidarity[3]. In Ukraine, this approach is also gradually gaining ground, but requires improvements to the mechanisms for the physical protection and financial incentives for whistleblowers to enhance the effectiveness of uncovering hidden crimes.

A body of case law has developed in Ukrainian and international judicial practice that recognises various forms of neutralisation depending on the type of threat (Table 3).

Table 3. Systematisation of tactical methods for countering resistance based on an analysis of national and international case law (2022-2025)

Case/defendant (jurisdiction)	Type of countermeasure detected	The neutralisation tactics employed	Result/legal consequence
The case of former Minister of Ecology Mykola Zlochevsky[4] No. 991/1297/22 (Ukraine, HACC) – Article 27(3) and Article 369(4) of the Criminal Code of Ukraine	Attempted bribery (USD 6 million), obstruction of justice (forgery of a signature), evasion of investigation	Reconstruction of the crime scene; *In absentia*; Plea bargaining	Financial neutralisation: UAH 660 million for the Armed Forces of Ukraine, a fine, a non-custodial sentence
The case of the Krayan plant[5] involving G.L. Trukhanov, former mayor of Odessa, and others. No. 521/17260/18, 991/2550/22, 991/3016/23 (Ukraine, HACC) – Article 191(5), Article 364(2), Article 368(4), Article 369(3), Article 206-2(3) and Article 209(3) of the Criminal Code of Ukraine	Regional judicial protectionism, use of administrative resources to exert pressure	Appeal proceedings; increase in bail; deprivation of citizenship	Administrative neutralisation: removal from office, elimination of means of influence
The case of former Supreme Court Chairman Vsevolod Knyazev[6], No. 991/1692/24[7], 2024 (Ukraine, HACC) – Article 368(4) of the Criminal Code of Ukraine	Conspiracy ("backroom dealings"), discrediting the NS(R)D ("provocation")	Undercover infiltration; technical surveillance; parallel administrative pressure	Institutional neutralisation: dismissal from office, judicial validation of the agent's actions
U.S. v. Bankman-Fried[8] (USA)	Witness Tampering (pressure via the media), use of Signal/VPN	Complete isolation: revocation of bail, detention pending trial	Prevention of information leaks and influence on witnesses
U.S. v. Sterlingov/Bitcoin Fog (USA)	Technical obfuscation, use of mixers	Digital de-anonymisation: blockchain analysis, transaction reconstruction	The admissibility of heuristic analysis as evidence; a conviction.

[1] Act for the Better Protection of Whistleblowers. (2023, May). Retrieved from https://www.gesetze-im-internet.de/englisch_hinschg/englisch_hinschg.html.
[2] Directive (EU) No. 2019/1937 of the European Parliament and of the Council "On the Protection of Persons Who Report Breaches of Union Law". (2019, October). Retrieved from https://eur-lex.europa.eu/eli/dir/2019/1937/oj/eng.
[3] Act for the Better Protection of Whistleblowers. (2023, May). Retrieved from https://www.gesetze-im-internet.de/englisch_hinschg/englisch_hinschg.html.
[4] The case of former Minister of Ecology Mykola Zlochevsky. (2022, May). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52020000000000473.
[5] The case of the Krayan plant. (2021, March). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52016000000000411.
[6] The case of former Supreme Court Chairman Vsevolod Knyazev. (2024, March). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52023000000000202.
[7] Case No. 991/1692/24. (2025, November). Retrieved from https://reyestr.court.gov.ua/Review/131931145
[8] United States v. Samuel Bankman-Fried, a/k/a "SBF," 22 Cr. 673 (LAK). (2024, March). Retrieved from https://www.justice.gov/usao-sdny/united-states-v-samuel-bankman-fried-aka-sbf-22-cr-673-lak.

Table 3. Continued

Case/defendant (jurisdiction)	Type of countermeasure detected	The neutralisation tactics employed	Result/legal consequence
The EncroChat case[1] (Germany, Federal Court of Justice)	Use of cryptophones ("dark-tech"), end-to-end encryption	Mass digital interception: hacking of servers by a foreign intelligence service	Precedent regarding the admissibility of evidence obtained through a mass data breach
The Tandler case (Germany, Munich Regional Court I)	Offshore schemes, disguising bribes as consultancy fees	Fiscal neutralisation: Verständigung (settlement) with full forfeiture	"Economic sterilisation": confiscation of EUR 7.8 million in assets
The Wirecard case (Germany)	Complex offshore transactions, the risk of capital flight prior to sentencing	Pre-emptive asset seizure: "Extended confiscation" of management assets	Blocking attempts to withdraw funds, ensuring compensation for losses

Source: compiled by the author based on M. Bushuev (2022), K. Ott (2023), Operator of "Bitcoin Fog" sentenced to more than 12 years in prison for running notorious Darknet cryptocurrency mixer (2024)

International practice, in turn, demonstrates a rigorous strategy for responding procedurally to information warfare. In the case of United States v. Samuel Bankman-Fried[2], the court neutralised "Witness Tampering" (leaks of the witness's diaries to the media and via Signal) by revoking bail and placing the defendant in complete isolation, recognising the use of VPNs and encrypted chats as a form of obstruction of justice. As for digital evidence, courts are legalising methods of "digital de-anonymisation". In the Bitcoin Fog case (Operator of "Bitcoin Fog"…, 2024), the admissibility of heuristic blockchain analysis to overcome trace obfuscation technologies was recognised, and in the EncroChat[3] case, the German Federal Court confirmed the lawfulness of mass data interception, emphasising the primacy of the interests of justice over the confidentiality of "dark-tech" correspondence. Furthermore, the neutralisation strategy encompasses the property aspect. In the Wirecard case (Bushuev, 2022), the preventive seizure of assets through "extended confiscation" was legitimised to prevent their transfer to offshore accounts, and in the Andrea Tandler case (Ott, 2023), the concept of "economic sterilisation" of the offence was implemented, which entails the complete deprivation of the defendant's benefits from corrupt ties as a mandatory condition of the plea bargain.

An analysis of case law across three jurisdictions shows that courts tend to side with the prosecution regarding the application of intensive procedural measures (server hacking, revocation of bail, freezing of assets pending sentencing) if the investigation demonstrates that the countermeasures are organised and high-tech in nature. Case law serves not only as a filter for the admissibility of evidence but also as an indicator of the evolution of neutralisation tactics, which are shifting from forceful confrontation to intellectual and technological struggle and procedural compromises (Porter, 2021; Bushuev, 2022; Ott, 2023).

A comparative analysis of tactics for countering obstruction in the field of transnational financial investigations has highlighted the advisability of implementing US approaches. The practice of the US Department of Justice (DOJ) regarding the application of the Foreign Corrupt Practices Act of 1977 (FCPA)[4] is based on a "coercion to cooperate" tactic through a policy of corporate enforcement[5]. The American strategy consists of creating conditions under which

[1] CaseC-670/22, M.N. (EncroChat): Judgment of the Court (Grand Chamber) (request for a preliminary ruling from the Landgericht Berlin – Germany) – Criminal proceedings against M.N. (Reference for a preliminary ruling – Judicial cooperation in criminal matters – Directive 2014/41/EU – European Investigation Order (EIO) in criminal matters – Obtaining of evidence already in the possession of the competent authorities of the executing State – Conditions for issuing an EIO – Encrypted telecommunications service – EncroChat – Need for the decision of a judge – Use of evidence obtained in breach of EU law). (2024, April). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62022CA0670.

[2] United States v. Samuel Bankman-Fried, a/k/a "SBF," 22 Cr. 673 (LAK). (2024, March). Retrieved from https://www.justice.gov/usao-sdny/united-states-v-samuel-bankman-fried-aka-sbf-22-cr-673-lak.

[3] CaseC-670/22, M.N. (EncroChat): Judgment of the Court (Grand Chamber) (request for a preliminary ruling from the Landgericht Berlin – Germany) – Criminal proceedings against M.N. (Reference for a preliminary ruling – Judicial cooperation in criminal matters – Directive 2014/41/EU – European Investigation Order (EIO) in criminal matters – Obtaining of evidence already in the possession of the competent authorities of the executing State – Conditions for issuing an EIO – Encrypted telecommunications service – EncroChat – Need for the decision of a judge – Use of evidence obtained in breach of EU law). (2024, April). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62022CA0670.

[4] Foreign Corrupt Practices Act of 1977. (1977, December). Retrieved from https://www.govinfo.gov/content/pkg/COMPS-9569/pdf/COMPS-9569.pdf.

[5] 9-47.120 – FCPA Corporate Enforcement Policy. (2019, March). Retrieved from https://www.justice.gov/criminal/criminal-fraud/file/838416/dl.

it is more advantageous for corporations to conduct an internal investigation themselves, identify the guilty parties and disclose the scheme to law enforcement agencies, rather than face the risk of criminal prosecution and fines. This tactic effectively shifts the burden of gathering evidence onto the legal entity, neutralising its resistance and turning a potential adversary into a source of evidence. For Ukraine, adapting this approach through the institution of plea agreements is a promising way to overcome resistance in cases involving complex financial schemes and large business structures. Tactics for neutralising attempts to discredit investigation findings through external oversight mechanisms were also analysed. The 2024 Report of the National Anti-Corruption Bureau of Ukraine (NABU) emphasises that conducting an independent audit of NABU's activities is a complex task that often becomes the subject of political manipulation. Opponents attempt to use audit procedures to gain access to confidential case materials or to obstruct the agency's work. Effective neutrality in this regard requires the inclusion of recognised international experts on the committees, whose reputation acts as a safeguard against politically motivated conclusions.

Based on the study of tactics used to counteract obstruction of investigations into official crimes, recommendations have been formulated for improving law enforcement and judicial activities in Ukraine, which are grounded in the modelling of effective institutional and tactical solutions tested in international practice. One of the key problems with the current legal framework in Ukraine is the lack of full technical autonomy for anti-corruption bodies in the conduct of covert investigative (surveillance) operations. In particular, the NABU cannot intercept information from telecommunications networks and is forced to involve other law enforcement agencies, which creates institutional risks of information leaks and the exposure of covert investigative operations. In contrast, under the legal systems of the US and Germany, specialised pre-trial investigation bodies possess full operational autonomy and internal technical capabilities for intercepting information, subject to strict judicial oversight and internal audit, which minimises the risks of external interference. Although Part 4 of Article 263 of the Criminal Procedure Code of Ukraine[1] already grants authorised units of the NABU the right to independently intercept information from transport telecommunications networks, the actual implementation of this provision is still hampered by the lack of autonomous technical infrastructure and independent connection channels to telecommunications operators. In this regard, the priority is to ensure the NABU's full technical independence by deploying internal equipment to provide direct access to telecommunications networks without the involvement of other law enforcement agencies. Implementing such a model will eliminate the bureau's institutional dependence, neutralise the risks of leaks of official information during the technical preparation of covert investigative operations, and ensure genuine confidentiality of investigations into high-level corruption even before they enter the active phase.

The primary focus of countering such interference is to ensure the security of criminal proceedings materials. In Ukraine, traditional methods of storing case materials leave room for their physical destruction or falsification. In contrast, European Union member states actively utilise digital criminal proceedings management systems based on the principles of data immutability and full traceability of access. In this regard, it is advisable to further scale up the "iCase" electronic criminal proceedings system, the legal foundation of which is already enshrined in Article 106-1 of the Criminal Procedure Code of Ukraine[2], which should become a priority in ensuring the technological level of countering obstruction. The full integration of this system into anti-corruption investigations guarantees the absolute inviolability of case materials. Thanks to the digital recording of every procedural action in real time, the risks of physical destruction, unauthorised removal or falsification of evidence are effectively eliminated, ensuring the integrity of the evidence base until it is presented to the court. The development of the institution of whistleblowers as a tool for internal neutralisation of countermeasures deserves particular attention. In Ukraine, mechanisms for the protection of whistleblowers remain insufficiently effective, which hinders the flow of information from within state bodies. In contrast, European Union countries are introducing secure internal reporting channels that guarantee anonymity and legal protection for individuals reporting corruption offences[3] (National Anti-Corruption Bureau of Ukraine, 2025). The introduction and proper functioning of such channels in Ukraine will help break down corporate solidarity within state bodies and ensure that evidence is obtained directly from within criminal schemes. In cases involving transnational corruption, it is advisable to make more active use of financial neutralisation tactics. In Ukraine, investigations often focus

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2] Ibidem, 2012.
[3] Act for the Better Protection of Whistleblowers. (2023, May). Retrieved from https://www.gesetze-im-internet.de/englisch_hinschg/englisch_hinschg.html.

on protracted procedural battles, whereas in US law enforcement practice, plea agreements with a focus on asset forfeiture and compensation for damages caused is prioritised[1]. Adapting this approach to the Ukrainian context will reduce the resources available to suspects for resistance and deprive them of the financial basis for further obstruction of the investigation. At the tactical level, the neutralisation of digital conspiracy is of paramount importance. In Ukraine, there is still no established judicial position on the admissibility of evidence obtained through high-tech access to digital information. At the same time, judicial practice in the EU and the US recognises the admissibility of evidence obtained through the analysis of encrypted communications and blockchain transactions, as a response to criminals' use of "dark-tech" tools[2] (Operator of "Bitcoin Fog"…, 2024). The adoption of a similar approach – which involves recognising the legitimacy of data obtained through the authorised circumvention of the cryptographic protection of specialised messaging apps and the de-anonymisation of digital asset holders using digital forensics and the analysis of public blockchain ledgers – in Ukrainian judicial practice will help prevent the use of digital technologies as a tool to obstruct investigations. The implementation of the proposed recommendations ensures a shift from reactively addressing the consequences of obstruction to proactively neutralising the risks of obstruction of justice in the investigation of official crimes.

To summarise, it is possible to argue that modern tactics for countering obstruction of investigations into official misconduct constitute a multi-layered system. They are not limited to the procedural actions of the investigator at the scene of the incident, but encompass institutional safeguards, strategic communications and international cooperation. Empirical data confirm that successfully overcoming resistance from corrupt elites is only possible if the institutional independence of the pre-trial investigation body is preserved and effective legislative mechanisms are in place to provide physical and legal protection for its staff against external interference.

Discussion

The findings of the study confirmed that, in the context of modern high-tech and institutionally entrenched corruption, the traditional paradigm of "overcoming" obstacles (as a reactive response to barriers that have already been created) is losing its effectiveness. Instead, the strategy of "neutralisation" has become the only viable direction for the development of investigative methods; this involves the preventive elimination of threats – financial, administrative and informational – before they can be irreversibly realised. The data obtained on the evolution of tactics in court cases demonstrated a shift from forceful confrontation to an intellectual and technological struggle. This observation correlates with the findings of D. Rothe & D. Kauzlarich (2022), who emphasised that crimes committed by public officials remain largely invisible or are reclassified as errors precisely because of the elites' ability to manipulate social control. These findings expand upon this thesis by demonstrating that Ukrainian practice has developed mechanisms (in particular, the institution of *in absentia* proceedings and plea agreements) that make these crimes "visible" and punishable even when the accused have fled, effectively neutralising the strategy of "invisibility" described by American researchers.

A key aspect identified during the study was the tactical nature of resistance to the investigation. As noted by V. Jitariuc (2023), the process of investigating corruption offences is inevitably accompanied by active resistance from criminals and their associates, leading to numerous errors on the part of the investigating authorities. This study confirmed this view using the example of The case of the Krayan plant[3][4], where the prosecution's initial tactics proved ineffective due to manifestations of local judicial subjectivity. However, in contrast to the author's identification of the problem, the results of this study revealed the existence of effective solutions. In particular, the application of appellate review by the High Administrative Court and administrative measures (deprivation of citizenship) serves as an effective tool for neutralising such resistance. This is consistent with the position of R.M. Jacobs (2022), who, using the example of the Republic of South Africa (RSA), justified the need to transition to an intelligence-led approach. In this case, the analysis of Case No. 991/1692/24[5] (the use of a notary as an agent) illustrated the successful implementation of precisely such an intelligence-led approach, which made it possible to neutralise the

[1] U.S. Code: Title 18 – Crimes and Criminal Procedure. (1948, June). Retrieved from https://www.law.cornell.edu/uscode/text/18.
[2] CaseC-670/22, M.N. (EncroChat): Judgment of the Court (Grand Chamber) (request for a preliminary ruling from the Landgericht Berlin – Germany) – Criminal proceedings against M.N. (Reference for a preliminary ruling – Judicial cooperation in criminal matters – Directive 2014/41/EU – European Investigation Order (EIO) in criminal matters – Obtaining of evidence already in the possession of the competent authorities of the executing State – Conditions for issuing an EIO – Encrypted telecommunications service – EncroChat – Need for the decision of a judge – Use of evidence obtained in breach of EU law). (2024, April). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62022CA0670.
[3] The case of the Krayan plant. (2021, March). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52016000000000411.
[4] Case No. 521/17260/18. (2019, July). Retrieved from https://clarity-project.info/court/decision/82973002.
[5] Case No. 991/1692/24. (2025, November). Retrieved from https://reyestr.court.gov.ua/Review/131931145.

"back-office" conspiracy at the very planning stage of the crime.

The academic literature extensively discusses the neutralisation techniques employed by criminals themselves to justify their actions. In their study of interviews with convicted fraudsters, M. Hoekstra *et al.* (2026) identified techniques such as denial of responsibility and the condemnation of those who condemn them. Similar conclusions were reached by S. Lazarus *et al.* (2026) when analysing cyber fraudsters who justify their crimes by citing historical injustice. This study revealed a mirroring trend. Investigators' tactics regarding "neutralising resistance" are, in fact, a response to the "guilt neutralisation techniques" employed by criminals. For example, in case No. 991/1297/22[1], the defendants attempted to "buy" the closure of the case, rationalising this as a routine business transaction (denial of harm), however, the investigation, through financial neutralisation (channelling funds towards Ukraine's defence), dismantled this construct, transforming the bribery attempt into a resource for the state. This approach resonates with the study by H.N. Pontell *et al.* (2021), who described how the Trump administration used the technique of "normalising the condemnation of prosecutors" to combat investigations. The Ukrainian experience (the Trukhanov case[2] [3]) has shown that the best response to such political rhetoric is procedural decisions (increasing bail), which shift the conflict from the political to the legal sphere.

The institutional aspect of neutralising resistance, examined in this study through the lens of the activities of the NABU and the HACC, engages with the conclusions of K. Bolkvadze (2025). The author argued that in hybrid regimes, to which the author classifies Ukraine during the period 2013-2019, elites have strong incentives to maintain corruption within law enforcement agencies as a tool for survival. However, the findings regarding the dynamics of 2022-2025 refute this thesis for the current period. The rise in the number of suspicions and a threefold increase in cases of detention indicate a shift from a "corruption pyramid" to a model of actively neutralising elite resistance. This correlates with the position of J. Cifuentes-Faura (2025), who, using the example of the war in Ukraine, demonstrated that transparency and digitalisation significantly reduce information asymmetry and increase government accountability even in crisis conditions.

The comparative analysis conducted in this study has revealed profound parallels between Ukrainian practice and international standards. J. Lenz (2025), analysing the selective application of international law by Western states (the USA, Germany), noted that national interests often take precedence over international legal obligations. However, the results of this study point to a reverse trend in Ukraine: the implementation of *in absentia* proceedings and *plea bargaining* (as in Case No. 991/1297/22[4]) demonstrated the priority of substantive liability and the inevitability of punishment over political expediency. This confirms the view of Ž. Navickienė *et al.* (2025) state that the planning of investigations into modern financial crimes has evolved outside narrow algorithms and now requires complex international neutralisation schemes that extend to the level of joint investigation teams.

A separate area of discussion concerns the evidential value of neutralisation measures. V. Gribincea (2025) emphasised that, when investigating latent corruption offences, the court tends to rely more on the results of covert investigative (or intelligence-gathering) operations (C(I)O) than on witness testimony. The latter are presented in the form of digital forensic reports (for example, automated data extraction logs, traffic log files or big data analysis reports), which ensures a high level of objectivity and verifiability of the evidence base. This study has confirmed this trend: the neutralisation of the "digital alibi" through the hacking of messaging apps and blockchain analysis (as in the EncroChat[5] or Bitcoin Fog cases (Operator of "Bitcoin Fog"…, 2024)) is becoming the foundation of the prosecution. At the same time, the concept of neutralisation proposed in this work is theoretically justified by M.A. Nuryanta *et al.* (2025). The authors described a paradigm shift from "formal truth" to "material truth" in pre-trial proceedings. Whereas previously the investigation was limited to the formal removal of obstacles, as of 2025, active measures (preventive seizure of assets, restriction of the subjective rights of suspects through judicial oversight) are aimed at establishing the facts during the investigation.

[1] The case of former Supreme Court Chairman Vsevolod Knyazev. (2024, March). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52023000000000202.
[2] Case No. 521/17260/18. (2019, July). Retrieved from https://clarity-project.info/court/decision/82973002.
[3] The case of the Krayan plant. (2021, March). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52016000000000411.
[4] The case of former Supreme Court Chairman Vsevolod Knyazev. (2024, March). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52023000000000202.
[5] CaseC-670/22, M.N. (EncroChat): Judgment of the Court (Grand Chamber) (request for a preliminary ruling from the Landgericht Berlin – Germany) – Criminal proceedings against M.N. (Reference for a preliminary ruling – Judicial cooperation in criminal matters – Directive 2014/41/EU – European Investigation Order (EIO) in criminal matters – Obtaining of evidence already in the possession of the competent authorities of the executing State – Conditions for issuing an EIO – Encrypted telecommunications service – EncroChat – Need for the decision of a judge – Use of evidence obtained in breach of EU law). (2024, April). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62022CA0670.

As regards the specific nature of white-collar crime, the findings of this study concerning the use of complex offshore schemes are fully consistent with the conclusions of T.A. Omang *et al.* (2024). The authors noted that corporate crimes, such as money laundering and bribery, have become an "epidemic" due to loopholes in legislation that are used by high-ranking officials to evade accountability. This study has demonstrated that judicial practice has begun to fill these gaps by legalising heuristic blockchain analysis as evidence. This is a critical step towards neutralising technological obfuscation of traces, as discussed by T.A. Omang *et al.* Furthermore, J. Cortese's (2022) work on public corruption in the US highlighted the link between corrupt officials and organised criminal networks. An analysis of "The case of the Krayan plant"[1] [2] confirmed the existence of such enduring links in Ukraine as well, where municipal property was being divested in favour of private entities through controlled individuals, requiring investigators to employ comprehensive tactics to neutralise the entire criminal organisation, rather than merely individual perpetrators.

It is also worth considering the cultural context of corruption, as explored by K. Artello & J.S. Albanese (2022). They argued that criminal prosecutions alone are insufficient to change the "culture of corruption", as local history and leadership have a decisive influence. These findings partly confirm this: despite successful cases of neutralisation, systemic resistance persists, transforming into new forms (legislative spam, media attacks). This suggests that neutralisation tactics must be complemented by a strategy of cultural change, as also noted by F. Ceschel *et al.* (2022), who emphasised the significance of a risk-oriented approach in the public sector.

The global context described in the textbook by F. Pakes (2024) on comparative criminal justice is noteworthy. The author analysed global trends such as the "punitive turn" and transnational policing. This study illustrated how these trends are implemented in practice. The EncroChat[3] case is an example of transnational neutralisation, where law enforcement agencies in one country (France) provide evidence to convict criminals in another (Germany), overcoming jurisdictional barriers. This opens new prospects for further research into the harmonisation of criminal procedure between the EU and Ukraine, particularly regarding the admissibility of digital evidence obtained by foreign partners. To summarise the discussion, it is possible to state that the doctrinal distinction between "overcoming" and "neutralisation" proposed in this study is not a purely theoretical construct but reflects real changes in crime-fighting tactics. The results of the analysis of judicial practice in Ukraine, the US and Germany indicate the formation of a common transatlantic standard. Effective investigation of white-collar crime is impossible without proactive measures aimed at depriving suspects of the resources (funds, positions, citizenship, technical means) they use to obstruct justice.

Conclusions

As a result of the research, the stated objective of distinguishing between the concepts of "overcoming" and "neutralising" resistance has been achieved, and the tactical tools for responding to threats during the investigation of corruption-related criminal offences have been systematised. A comprehensive analysis of sources, the regulatory framework and law enforcement practice formed several generalised scientific and practical conclusions. The study established that the tendency in legal doctrine to equate the terms "overcoming" and "neutralisation" is erroneous and reduces the effectiveness of investigative activities in the context of hybrid threats. The study demonstrated that the category of "overcoming" is retrospective in nature and aimed at removing obstacles that have already arisen, such as the restoration of destroyed documentation or the re-examination of witnesses. Such an approach requires significant time and material resources and does not guarantee the restoration of the evidence base to its original state. In contrast, "neutralisation" is defined as a proactive strategy, the essence of which lies in balancing forces or bringing the threat under control before irreversible consequences occur. A paradigm shift in the investigation of official crimes has been noted. There is a shift in focus from the physical seizure of data storage media to the intellectual and technological blocking of a suspect's ability to resist using administrative or financial resources.

A systematic analysis of judicial practice in Ukraine, the US and Germany has confirmed the effectiveness of a three-tiered neutralisation system: procedural, financial and technological. A key indicator of this model's effectiveness is the increasing number of cases in which courts have legalised the

[1] The case of the Krayan plant. (2021, March). Retrieved from https://hacc-decided.ti-ukraine.org/uk/cases/52016000000000411.
[2] Case No. 521/17260/18. (2019, July). Retrieved from https://clarity-project.info/court/decision/82973002.
[3] CaseC-670/22, M.N. (EncroChat): Judgment of the Court (Grand Chamber) (request for a preliminary ruling from the Landgericht Berlin – Germany) – Criminal proceedings against M.N. (Reference for a preliminary ruling – Judicial cooperation in criminal matters – Directive 2014/41/EU – European Investigation Order (EIO) in criminal matters – Obtaining of evidence already in the possession of the competent authorities of the executing State – Conditions for issuing an EIO – Encrypted telecommunications service – EncroChat – Need for the decision of a judge – Use of evidence obtained in breach of EU law). (2024, April). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62022CA0670.

tactic of "compromise neutralisation" through plea agreements. Empirical data, in particular the results of the case concerning an attempt to bribe the leadership of anti-corruption bodies, demonstrate that the application of this tactic has channelled over UAH 660 million into the state budget. This indicates a shift in the national legal system from a purely punitive model towards a pragmatic approach of "economic sterilisation" of crime. Under this approach, the priority is not merely the isolation of the individual – which may be complicated under remote justice conditions – but the complete deprivation of the corrupt official's financial basis for further resistance. In addition to the financial aspect, a trend towards strengthening measures to neutralise administrative resources has been identified, as evidenced by precedents involving the application of preventive measures and the revocation of citizenship from individuals who use dual status to evade accountability. The ability of pre-trial investigation bodies to conduct digital de-anonymisation has been identified as a key factor in the success of the fight against high-tech corruption. A review of international case law concerning the use of crypto-phones and cryptocurrency mixers has demonstrated that courts are prepared to accept as admissible evidence obtained through the mass breach of cryptographic security and heuristic analysis of the blockchain. For the Ukrainian legal system, this highlights the need to implement similar technical approaches and legislative regulation of the use of specialised software for covert access to secure systems, which will help to neutralise the technological advantage of organised criminal groups.

A promising area for further research is the exploration of ways to integrate artificial intelligence into the process of identifying signs of preparations for countermeasures, in particular the analysis of anomalous activity involving assets before investigative actions. It is also necessary to develop tactics for neutralising threats associated with the use of deepfake technology, which poses new challenges for the verification of evidence.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Amelin, O.Yu. (2025a). Search of a person as a way of collecting evidence in the pre-trial investigation of accepting an offer, promise or receiving of an illegal benefit by an official. *Constitutional State*, 58, 220-231. doi: 10.18524/2411-2054.2025.58.331008.

[2] Artello, K., & Albanese, J.S. (2022). Culture of corruption: Prosecutions, persistence, and desistence. *Public Integrity*, 24(2), 142-161. doi: 10.1080/10999922.2021.1881300.

[3] Benson, M.L., Simpson, S.S., Rorie, M., & Kennedy, J.P. (2024). *White-collar crime: An opportunity perspective*. New York: Routledge. doi: 10.4324/9781003175322.

[4] Bolkvadze, K. (2025). Corrupt or repressive? How political competition incentivizes hybrid regimes to subvert police in distinct ways. *Governance*, 38(3), article number e70030. doi: 10.1111/gove.70030.

[5] Boreiko, H., & Navrotska, V. (2023). Abuse of the right to prosecution in criminal proceedings: The experience of Ukraine and the United States. *Social and Legal Studios*, 6(4), 38-47. doi: 10.32518/sals4.2023.38.

[6] Bushuev, M. (2022). *Wirecard: Financial scandal in Germany reaches court*. Retrieved from https://www.dw.com/uk/wirecard-finansovij-skandal-stolitta-v-nimeccini-dijsov-do-sudu/a-64029607.

[7] Ceschel, F., Hinna, A., & Homberg, F. (2022). Public sector strategies in curbing corruption: A review of the literature. *Public Organization Review*, 22(3), 571-591. doi: 10.1007/s11115-022-00639-4.

[8] Cherniei, V., Cherniavskyi, S., Babanina, V., & Ivashchenko, V. (2022). Criminal remedies and institutional mechanisms for combating corruption crimes: The experience of Ukraine and international approaches. *Juridical Tribune*, 12(2), 227-245. doi: 10.24818/TBJ/2022/12/2.05.

[9] Cifuentes-Faura, J. (2025). The role of accountability and transparency in government during disasters: The case of Ukraine-Russia war. *Public Money & Management*, 45(3), 256-265. doi: 10.1080/09540962.2023.2243131.

[10] Cortese, J. (2022). *Public corruption in the United States: analysis of a destructive phenomenon*. New York: Routledge. doi: 10.4324/9781003197447.

[11] European Union Agency for Criminal Justice Cooperation. (2024). *Eurojust consolidated annual activity report 2023*. Retrieved from https://www.eurojust.europa.eu/publication/eurojust-consolidated-annual-activity-report-2023.

[12] Gavoor, A.A., & Platt, S.A. (2022). Administrative investigations. *Indiana Law Journal*, 97(2), article number 1.

[13] Gottschalk, P. (2024). Investigating and prosecuting white-collar and corporate crime: Challenges and barriers for national police agencies. *Journal of Economic Criminology*, 3, article number100051. doi: 10.1016/j.jeconc.2024.100051.
[14] Gribincea, V. (2025). The use of investigative information during the judicial examination stage of the criminal cases. *Law and Life*, S, 251-258.
[15] Hoekstra, M., Huisman, W., & van der Schee, B. (2026). Catching neutralizations: Identifying neutralization techniques for white-collar crimes in offender statements. *Journal of Economic Criminology*, 11, article number 100203. doi: 10.1016/j.jeconc.2025.100203.
[16] Jacobs, R.M. (2022). *Exploring the use of tactical crime intelligence techniques in corruption investigations*. Pretoria: University of South Africa.
[17] Jitariuc, V. (2023). Tactical particulars regarding the conduct of criminal prosecution at the initial and subsequent stage of the investigation of corruption crimes. *Scientific Bulletin of the "Bogdan Petriceicu Hasdeu" State University of Cahul: Social Sciences*, 17(2), 35-47. doi: 10.5281/zenodo.10438583.
[18] Kassimova, M.O., Omarov, Y.A., Zhilkaidarov, R.R., Abulgazin, Y.S., & Sabitova, A.A. (2023). Investigative prevention of corruption crimes. *Journal of Financial Crime,* 30(1), 254-265. doi: 10.1108/JFC-11-2021-0252.
[19] Krykunov, O., Kondratishyna, V., Starko, O., Tserkunyk, L., & Kravets, Y. (2023). Prevention and overcoming of counteraction to the investigation of crimes committed against participants in criminal proceedings. *Political Issues*, 41(76), 901-917. doi: 10.46398/cuestpol.4176.53.
[20] Lazarus, S., Hughes, M., Button, M., & Garba, K.H. (2026). Fraud as legitimate retribution for colonial injustice: Neutralization techniques in interviews with police and online romance fraud offenders. *Deviant Behavior*, 47(3), 427-448. doi: 10.1080/01639625.2024.2446328.
[21] Lenz, J. (2025). *A shame on our shared humanity: A qualitative comparative case study of selective application of international law by Western states*. Lund: Lund University.
[22] Majid, K., & Kapure, A. (2025). *Neutralization techniques in law enforcement interviews: How fraudsters rationalize crime*. Retrieved from https://www.researchgate.net/profile/Anil-Kapure/publication/389992445 pdf.
[23] National Anti-Corruption Bureau of Ukraine. (2024). *Report: First half of 2024*. Retrieved from https://nabu.gov.ua/activity/reports/pershe-pivrichchia-2024-roku/.
[24] National Anti-Corruption Bureau of Ukraine. (2025). *Report: First half of 2025*. Retrieved from https://nabu.gov.ua/activity/reports/pershe-pivrichchia-2025-roku/.
[25] Navickienė, Ž., Krikščiūnas, R., Bilius, M., & Milienė, D. (2025). Modern discourse on financial crime pre-trial investigation planning. *Baltic Yearbook of International Law Online*, 23(1), 180-198.
[26] Nuryanta, M.A., Hartiwiningsih, H., Suwadi, P., & Frimanda, N. (2025). Shift in pre-trial procedural law: a study using paradigm theory. *International Conference on Law, Technology, Spirituality and Society,* 5, 50-64.
[27] Office of the Attorney General. (n.d.). *About persons who have committed criminal offenses*. Retrieved from https://gp.gov.ua/ua/posts/pro-osib-yaki-vcinili-kriminalni-pravoporusennya-2.
[28] Official statement of NABU and SAPO regarding draft law No. 12414. (2025). Retrieved from https://nabu.gov.ua/news/ofitciyina-zaiava-nabu-i-sap-shchodo-zakonoproyektu-12414/.
[29] Omang, T.A., Ojong-Ejoh, M.U., Uzoh, E.E.C., Agwanwo, D.E., Onyejegbu, D.C., Okemini, O.O., Obiefuna, O., & Egwu, F.O. (2024). White-collar crimes in Uganda: Exploring the impacts and strategies for reform. *Journal of Somali Studies*, 11(3), 117-137. doi: 10.31920/2056-5682/2024/v11n3a6.
[30] Operator of "Bitcoin Fog" sentenced to more than 12 years in prison for running notorious Darknet cryptocurrency mixer. (2024). Retrieved from https://www.justice.gov/usao-dc/pr/operator-bitcoin-fog-sentenced-more-12-years-prison-running-notorious-darknet.
[31] Ott, K. (2023). *Tax investigation report heavily implicates mask millionaire Tandler*. Retrieved from https://www.sueddeutsche.de/bayern/andrea-tandler-maskenaffaere-steuerfahndung-schweiz-festnahme-fluchtgefahr-1.5744537?reduced=true.
[32] Pakes, F. (2024). *Comparative criminal justice*. London: Routledge. doi: 10.4324/9781003390688.
[33] Patrikeeva, N. (2025). *Zelensky signed the scandalous law No. 12414*. Retrieved from https://www.bbc.com/ukrainian/articles/cgeqllep70no.
[34] Pontell, H.N., Tillman, R., & Ghazi-Tehrani, A.K. (2021). In-your-face Watergate: Neutralizing government lawbreaking and the war against white-collar crime. *Crime, Law and Social Change*, 75(3), 201-219. doi: 10.1007/s10611-021-09954-1.
[35] Porter, L.E. (2021). Police misconduct. In R.G. Duhman, G.P. Alpert & K.D. McLean (Eds.), *Critical issues in policing: Contemporary readings (*pp. 261-278). Long Grove: Waveland Press, Inc.

[36] Puddister, K., & McNabb, D. (2021). When the police break the law: The investigation, prosecution and sentencing of Ontario police officers. *Canadian Journal of Law and Society*, 36(3), 381-404. doi: 10.1017/cls.2021.3.
[37] Rothe, D., & Kauzlarich, D. (2022). *Crimes of the powerful: White-collar crime and beyond*. London: Routledge. doi: 10.4324/9781003124603.
[38] Stepaniuk, R. (2025). Digital forensics and its importance in investigating criminal offences. *Bulletin of the Penitentiary Association of Ukraine*, 3, 181-192. doi: 10.34015/2523-4552.2025.3.20.
[39] Tarkan, O. (2025). Activity nature of counteracting investigation of criminal offenses. *Theory and Practice of Forensic Science and Criminalistics*, 39(2), 148-161. doi: 10.32353/khrife.2.2025.11.
[40] Tsutskiridze, M.S. (2020). *Criminal procedural activities of the investigator: Theory and practice of evidence*. Kyiv: Alert.
[41] United Nations Office on Drugs and Crime. (2025). *Guidance Note for States parties on sharing information and experiences on protection of whistle-blowers and other reporting persons*. Retrieved from https://track.unodc.org/uploads/documents/UNCAC/WorkingGroups/workinggroup4/2025-June-17-20/Contributions-whistler-blower/Ukraine_English.pdf.

Тактика нейтралізації протидії досудовому розслідуванню кримінальних правопорушень у сфері службової діяльності

Олександр Амелін
Кандидат юридичних наук, доцент
Офіс Генерального прокурора
01011, вул. Різницька, 13/15, м. Київ, Україна
Навчально-науковий інститут права Державного податкового університету
08201, вул. Університетська, 31, м. Ірпінь, Україна
https://orcid.org/0000-0002-0933-2111

■ **Анотація.** Метою роботи було визначення алгоритмів нейтралізації протидії та розробка системи тактичних прийомів для захисту досудового розслідування службових злочинів від деструктивного впливу. Підґрунтям дослідження було поєднання порівняльно-правового аналізу, кількісного опрацювання офіційних статистичних даних, якісного аналізу судової та слідчої практики. На основі порівняльно-правового аналізу законодавства й прецедентів України, Сполучених Штатів Америки та Федеративної Республіки Німеччина здійснено систематизацію інструментів нейтралізації та подолання опору спеціальних суб'єктів. Встановлено, що на відміну від ретроспективного подолання стратегія нівелювання загроз передбачає випереджальне блокування адміністративних і фінансових ресурсів підозрюваного до настання незворотних наслідків. За результатами аналізу емпіричних даних підтверджено ефективність трирівневої системи реагування на протидію розслідуванню, яка передбачає поєднання фінансових, технологічних і процесуальних заходів. Визначено, що пріоритетним вектором є позбавлення посадовця економічної вигоди, що підтверджується практикою арешту активів у іноземних юрисдикціях і застосуванням інституту угод. Доведено дієвість використання масового дешифрування захищених месенджерів та аналізу блокчейну для виявлення прихованих зв'язків у високотехнологічних схемах із залученням криптовалютних міксерів. Наукова робота підтверджує необхідність імплементації міжнародних стандартів відповідальності за втручання в правосуддя й розширення повноважень антикорупційних органів щодо автономного перехоплення інформації з телекомунікаційних мереж для мінімізації витоків. Практична цінність отриманих результатів полягає в можливості безпосереднього використання запропонованих рекомендацій для вдосконалення кримінального процесуального законодавства

■ **Ключові слова:** вплив; тиск; загрози; подолання; докази; арешт майна; угоди про визнання винуватості; обшук; слідчі дії; службові злочини; корупція; судова практика