Can hacking be ethical: A legal review

Valeriia Filinovych[1,*,†], Assel Mukasheva[2,†]

[1]Scientific Cyber Security Association of Ukraine, Mykhaila Dontsia Str., 2A, Kyiv, 03161, Ukraine
[2]Kazakh-British Technical University, Tole Bi Str., 59, Almaty, 050000, Kazakhstan

Abstract

The concept of ethical hacking and its legal status in the Ukrainian legal system compared to international approaches is researched in this article. Although organizations often engage pen testers to identify vulnerabilities in their systems, their activities raise complex legal issues, especially in jurisdictions with no clear regulatory framework. The study analyzes Ukrainian legislation, particularly Article 361 of the Criminal Code. It compares it with relevant norms of the United States and the European Union, such as the Computer Fraud and Abuse Act and the NIS2 Directive. It is shown that Ukraine does not explicitly prohibit penetration testing, but it does not have a comprehensive legal framework to regulate such activities. The paper emphasizes the urgent need to define the legal status of ethical hackers, establish activity standards, and implement regulatory safeguards. In war conditions and the growth of cyber threats, legal clarity and structured mechanisms for cybersecurity testing have become crucial for Ukraine's national security and resilience.

Keywords

hacking, ethical hacker, penetration testing, cybersecurity law, white hat hackers, NIS2 Directive, Computer Fraud and Abuse Act, legal regulation,

1. Introduction

At the end of 2025, the Cyber Police Department of the National Police of Ukraine published a report, according to which the most common cyber threats continue to be phishing, online fraud, database theft, interference with the work of web resources, and the like [1]. Quite often, the reason for this is technical and organizational vulnerabilities, such as insufficient system protection, software vulnerabilities, and incorrect access management. Of course, the human factor also plays an important role in this.

What can companies do to prevent this from happening? Of course, it is always necessary to start with a well-developed cybersecurity policy at the enterprise, as well as staff training. It is also important to search for vulnerabilities in the systems themselves. For this, business entities increasingly turn to "ethical hackers" for help. However, can hacking be considered legal? In this article, we will answer the question posed.

Nevertheless, its basic concepts should be defined before proceeding to the regulatory support of such a topic.

Thus, hacking, according to the definition of A. Gupta and A. Anand, is a technique for searching for loopholes and weak spots in ICT systems and networks with the subsequent use of such "soft spots" for unscrupulous purposes (in particular, obtaining unauthorized access to certain information, modifying the functions of systems or networks, and the like). That is, the subject committing the act of hacking pursues clearly different goals than those of an ordinary user [2]. Accordingly, a hacker is a person who commits the actions mentioned.

The previous formulation clearly indicates the unscrupulousness of the hacker's goals. However, does he always act unscrupulous, and can his actions sometimes be helpful for companies and other business entities?

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

*Corresponding author.
†These authors contributed equally.
vvfilinovich@gmail.com (V. Filinovych); a.mukasheva@gmail.com (A. Mukasheva)
0000-0001-8824-615X (V. Filinovych); 0000-0001-9890-4910 (A. Mukasheva)

Table 1
Comparison of Types of Hackers

	White Hat Hacker	Grey Hat Hacker	Black Hat Hacker
Legality of Activity	Legal and authorized	Semi-legal	Unethical and illegal
Purpose of Activity	Hired to find holes and vulnerabilities	Cannot be clearly called bad; typically act due to ideological reasons or "for fun"	Act with a negative, malicious purpose
Motivation	Professional activity; legal and ethical motivation	Disagreement with political position or company policy; entertainment	Usually economic incentives; less often – revenge, gaining popularity
Typical Actions	Penetration testing, vulnerability scanning with permission	Hack without permission, then disclose vulnerabilities found	Destroy data, disable systems, violate organizational confidentiality/integrity
Other titles	*Ethical hackers*	*Hacktivists*	*Crackers*

Today, many types of hacking are known, and, accordingly, types of hackers. Thus, 10Guards, in particular, lists 15 such "specialists" (from black hackers to botnet hackers) [3]. According to the definition of the already mentioned A. Gupta and A. Anand, there are three main ones - black, gray and white (Black Hat Hackers, Grey Hat Hackers, White Hat Hackers) [2]. Zoran Cekerevac and others came to a similar classification, who, in particular, note that both motivated women and men with basic knowledge and desire, as well as a large reserve of patience and the ability to plan goals, can engage in hacking, depending on the "classification" such individuals can pursue different goals [1, 4]. Saachi Joshi also divides them into three types "by color" [5].

Summarizing the existing approaches [5, 6, 7, 8] to the identification of types of hackers, we note the following:

- black hackers - always act with a negative, malicious purpose, usually with economic incentives (less often - for revenge, gaining popularity, and the like.), they are also called crackers. These attackers try to penetrate a protected network to destroy data, turn off the network, etc. Unethical offenders often violate the confidentiality, integrity, or availability of systems and data of a company or other organization;
- gray hackers - they cannot be unequivocally called bad guys. Usually, their goal is ideological motives (for example, speaking out against a hostile political position or company policy alien to them) or "have fun." They are often known as hacktivists. That is, they do not pursue a negative goal but do not have the appropriate permissions to access information, communication systems, and networks. Usually, they inform the hacked party about the vulnerabilities found;
- white hackers - they are specially hired to search for holes and other vulnerabilities. They are also called ethical hackers. They do not violate the law because access is provided to them directly by the owners, but the methods they use for testing are, in particular, the same as those of black hats (see Table 1).

In conclusion, we note that black hackers are clearly offenders, gray ones too, however, they do not have a useful purpose, but also act without appropriate permission, and white ones are specially hired individuals who commit hacking on behalf of the organization, network and system that needs to be tested for vulnerability. The latter and their activities are the subject matter of this article.

2. Summary of the primary material

White hats are hired to perform penetration testing. It is a comprehensive vulnerability testing, with a thorough analysis of the system, particularly for poor or incorrect system configuration, hardware, software deficiencies, and operational weaknesses in the process. Testers can suggest technical countermeasures [9, 10]. Therefore, ethical hackers are officially called pentesters.

In Ukraine, the attitude towards hacking is quite specific. The existing legislation does not define ethical or other types of hackers and generally does not fully regulate this area. An analysis of US and EU legislation indicates the absence of such definitions in relevant international entities.

In the context of this issue, the following regulatory acts should be mentioned as of our state: the Criminal Code of Ukraine, the Laws of Ukraine "On Information", "On Information Protection in Information and Communication Systems", "On the Basic Principles of Ensuring Cybersecurity in Ukraine", and the like.

Thus, Chapter XVI of the Criminal Code consists of six articles devoted to offenses in the field of using computers, systems, and networks.

- Its Article 361 regulates the issue of hacking and deals with unauthorized interference with the operation of computers, systems, and networks, for which a fine of 1-3 tax-free minimum incomes of citizens (hereinafter - TFMI), or from 1 to 3 years of restriction of liberty or probationary supervision (without isolation from society) is provided.
- If hackers commit such an offense by prior conspiracy or repeatedly, the fine will increase to 3-7 thousand TFMI or 2-5 years of restriction or imprisonment.
- If, as a result of the above actions, data is leaked, blocked, forged, or lost, then the fine increases to 7-10 thousand TFMI, and imprisonment will last 3-8 years; the guilty party may also be prohibited from working in certain positions and engaging in certain types of activities for a period of up to 3 years.
- The latter is also provided with imprisonment for 8-12 years if the relevant hacking caused the danger of serious man-made accidents or environmental disasters, death, or mass illness of people [11].

Given the martial law regime introduced in Ukraine, it is important to consider Part 5 of Article 361, which concerns cases 3 and 4 above. Accordingly, during such a period, the commission of the above actions will entail the imposition of liability on the guilty person in the form of imprisonment for 10-15 years [11]. These norms apply, first of all, to black and gray hats.

As for pentesters, there is a particular Part 6 of Article 361, which directly provides that the listed actions will not be considered unauthorized interference if they were committed “following the procedure for searching and identifying potential vulnerabilities of such systems or networks” [11] (see Figure 1).

For unauthorized actions with data on computers, systems, and networks, namely their modification, destruction, or blocking, as well as interception or copying, one can receive a fine in the amount of 2-4 thousand TFMI or be sent to 2 years of corrective labor or be deprived of liberty for a term of up to 3 years, respectively. Suppose such an act is committed again or by a group with prior consent or leads to significant damage. In that case, the punishment will be more serious - deprivation of liberty for 3-6 years. Such is provided for in Article 362 [11].

Table 2 below summarizes the sanctions mentioned, which are applicable to unauthorized interference and data manipulation as outlined in Articles 361 and 362 of the Criminal Code.

According to Article 20 of the Law on Information, the latter is divided into open and information with limited access. Article 21 clearly states that there is information with limited access, which is divided into official, secret, and confidential. Collecting, using, distributing, and storing the latter is prohibited. Nevertheless, there are exceptions: national security, protection of human rights, and economic well-being. Also, Article 29 allows the dissemination of information with limited access if it is a subject of public interest [12].

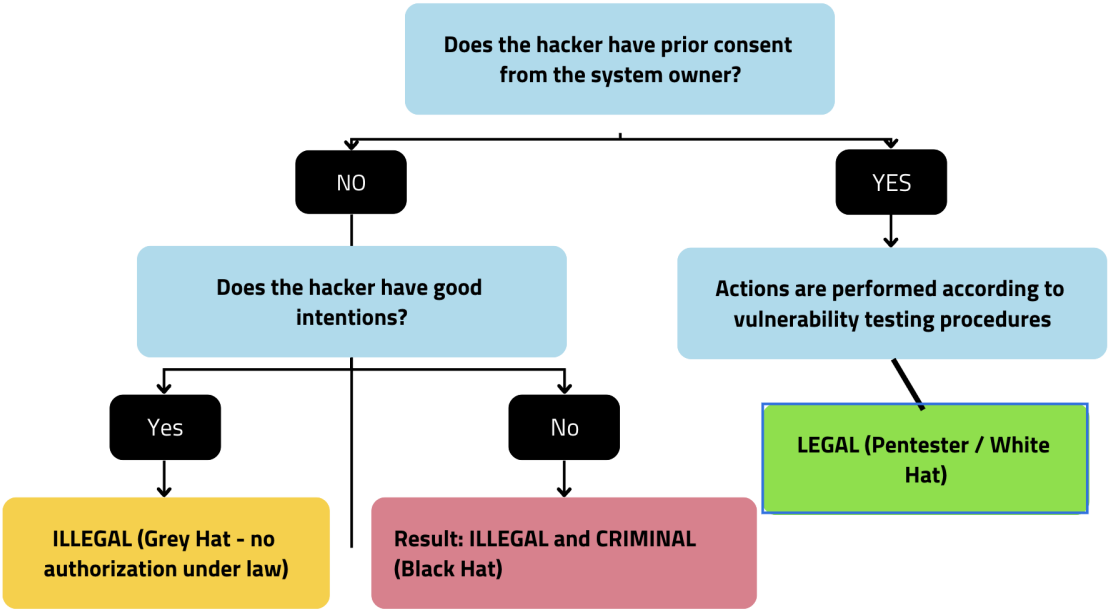

Figure 1: Legal status of hacking activities.

Article 1 of the Law on Information Protection in Information and Communication Systems defines unauthorized actions regarding information in the system. These are performed in violation of the established access procedure [13]. Accordingly, such actions can be called hacking.

According to Article 9 of the said law, the owner of the system or its administrator must ensure the protection of information in the system. According to Article 1, it is necessary to ensure information integrity, availability, and confidentiality. Article 11 imposes liability under the law on those guilty of the relevant violations [13]. That is, this law covers the activities of black and gray hats, and violations will be considered, in particular, disruption of work or unauthorized access to system resources, as well as the distribution of malicious programs. Therefore, the system must provide for the possibility of user identification and authentication, measures to counter potential threats, and registration of security events. The so-called Law on Cybersecurity (2163-VIII) defines the legal framework for cybersecurity but does not directly mention the terms "hacking," "pentester," or "ethical hacker." Nevertheless, the document contains several provisions directly related to countering hacking and regulating the possibility of lawful security testing.

Thus, Article 1 of the aforementioned Law defines a cyberattack as an example of hacking. These are targeted malicious actions in cyberspace using electronic communications, committed to violating the confidentiality, integrity, availability, or unauthorized access to electronic information resources, breaking the security and normal functioning of systems, or using such systems to carry out cyberattacks on other objects of protection in cyberspace. Article 10 of the Law provides for public-private interaction in the relevant field, which includes, in particular, the development and operation of a system for timely detection, prevention, and neutralization of threats in cyberspace, "including with the involvement of volunteer organizations" and interaction with individuals and organizations and companies to implement cyber defense measures [14]. That is, there is a permission to involve pentsters in checking systems. Three types of liability are provided for illegal actions: civil, administrative, and criminal.

In contrast, we will point to the experience of leading players in the international arena in this matter. As already noted above, the legislation of the United States also does not contain a legislative definition of ethical hacking. However, this practice has gained wide recognition in the cybersecurity community. The key American legal instrument, the Computer Fraud and Abuse Act, criminalizes

Table 2
Sanctions under the Criminal Code of Ukraine

Type of Offense	Article	Circumstances	Sanction
Unauthorized interference with systems	361(1)	Basic offense	Fine (1-3 TFMI) / 1-3 years of liberty restriction or probation
Repeat/conspiracy offense	361(2)	Aggravated circumstances	Fine (3-7 TFMI) / 2-5 years of liberty restriction or imprisonment
Data leak/block/-forgery/loss	361(3)	Consequential damage caused	Fine (7-10 TFMI) or 3-8 years imprisonment + optional disqualification (up to 3 years)
Severe consequences/significant damage	361(4)	Danger of man-made accident, environmental disaster, death, or mass illness	8-12 years imprisonment + optional disqualification (up to 3 years)
Severe consequences under martial law	361(5)	Under martial law – danger to public	10-15 years imprisonment + optional disqualification (up to 3 years)
Penetration testing with consent	361(6)	With prior authorization for testing	NOT punishable – exempted explicitly
Unauthorized data modification/destruction/blocking	362(1)	Basic offense	Fine (2-4 TFMI) / corrective labor (up to 2 years)
Unauthorized data interception/copying with leak	362(2)	Consequential damage caused	Up to 3 years imprisonment + disqualification (up to 3 years)
Repeat/group/significant damage	362(3)	Aggravated circumstances	3-6 years imprisonment + disqualification (up to 3 years)

exactly unauthorized access. Nevertheless, in practice, courts have already begun to distinguish between malicious hacking and authorized testing. The issue of pen testing is also affected to one degree or another by the norms of the following documents: Digital Millennium Copyright Act, Electronic Communications Privacy Act, Health Insurance Portability and Accountability Act, and Children's Online Privacy Protection Act [15].

Note: TFMI refers to Tax-Free Minimum Income (a unit used for calculating fines under Ukrainian law).

The European Union has a special NIS 2 Directive (Directive 2022/2555) that establishes measures to "achieve a high common level of cybersecurity across the Union" [15]. Although it does not contain the word "pentesting," it does provide for appropriate procedures.

Such a measure simulates a cyber attack on an organization's assets to identify vulnerabilities. Systems should be tested once a year after significant IT infrastructure changes or after cyber incidents. It is worth emphasizing that system testing is not a choice; it is a direct obligation under the Directive and applies, in particular, to essential entities (providing critical infrastructure), important entities (not critical but important for the economy), and non-European companies operating in the EU [16].

So, although Ukrainian legislation does not contain direct regulation of the activities of pentesters as a separate category of specialists, this issue is indirectly regulated. The situation is similar with gray and black hackers. Nevertheless, there is no direct ban on conducting pentesting, the main thing is that such relations are regulated at the contractual level between the company that needs to check the system for vulnerability, and the ethical hacker himself. Otherwise, his activities will already be

considered illegal.

We agree with Brian Smith, who insists on the following rules for pentesters:

- first of all, it is necessary to obtain written permission to conduct testing;
- clearly set limits on the scope of testing;
- perform all actions with maximum protection of Sensitive Data;
- avoid interception of communications;
- document all actions;
- provide high-quality reports on the results of testing [15].

For a visual perception of these steps, Figure 2 is presented below.

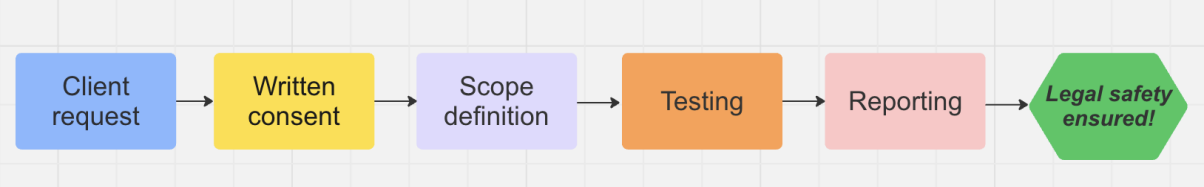

Figure 2: Roadmap for ethical pentesting.

Furthermore, from our side, we want to add the importance of absolutely following the current legislation of Ukraine.

3. Conclusions

Summing up the above, hacking activities can indeed be ethical and legal, but only if the owner of the system or network has previously granted permission for the relevant actions. Agreeing clearly on technical and legal aspects between the parties is mandatory. Otherwise, the tester's actions will be qualified as a criminal offense.

Ukrainian legislation does not sufficiently regulate this issue; it is fragmentary. However, the analysis of existing regulatory legal acts allowed us to identify the legal framework of ethical hacking. In particular, it was determined that, following Part 6 of Article 361 of the Criminal Code, the activities of pentesters, if they act with prior consent of the owner of the system or network, are legitimate.

Nevertheless, the existing legislation requires significant improvements; in particular, it is considered necessary to provide an official concept of ethical hacking, with a clear definition of the legal status of pentesters, and to develop and implement a standardized procedure for security testing. In this regard, for the sake of legal certainty and protection of the rights of the relevant parties, it is advisable to develop regulatory documents and instructions for conducting pentesting in the public and private sectors.

A separate document should be developed to determine the requirements for pentesters, particularly the qualifications, prerequisites, and rules for issuing written consent to conduct testing with a record of permitted actions. Also, a professional standard for ethical hackers in Ukraine is needed.

Finally, it is worth pointing out the importance of educational activities in society, both in the ethical aspects of hacking and in general, to raise awareness among citizens in cyber hygiene.

In this difficult time for Ukraine, when the enemy is everywhere using not only conventional methods of warfare but also cyber warfare means, a qualitative analysis of systems and networks for vulnerability, especially for critical infrastructure facilities, with the subsequent elimination of such "holes" can become the basis for obtaining significant advantages for our state.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] Cyber Police Department, Report on the activities of the cyber police department of the national police of ukraine in 2024, 2025. URL: https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/, accessed: 12.06.2025.

[2] A. Gupta, A. Anand, Ethical hacking and hacking attacks, International Journal of Engineering and Computer Science 6 (2017) 21042–21050. doi:10.18535/ijecs/v6i4.42.

[3] 10Guards, The thin line between cybercrime and ethical hacking – the 15 types of hackers you need to know in 2023, 2023. URL: https://10guards.com/, accessed: 12.06.2025.

[4] Z. Cekerevac, et al., Hacking, protection and the consequences of hacking, Communications - Scientific letters of the University of Zilina 20 (2018) 68–72. doi:10.26552/com.c.2018.2.83-87.

[5] S. Joshi, et al., Cybersecurity in the modern world: ethical hacking, International Research Journal of Modernization in Engineering Technology and Science 5 (2023) 1792–1798. doi:10.56726/irjmets44859.

[6] ScienceDirect, Black hat hacker, 2025. URL: https://www.sciencedirect.com/topics/computer-science/black-hat-hacker, accessed: 12.06.2025.

[7] J. Gaia, et al., Psychological profiling of hacking potential, in: Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020, pp. 2230–2239. URL: http://hdl.handle.net/10125/64014.

[8] K. Zetter, Hacker lexicon: what are white hat, gray hat, and black hat hackers?, WIRED, ???? URL: https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/, accessed: 12.06.2025.

[9] A. G. Bacudio, et al., An overview of penetration testing, International Journal of Network Security & Its Applications 3 (2011) 19–38. doi:10.5121/ijnsa.2011.3602.

[10] S. Mirza, Nis 2 penetration testing, Cyphere, 2024. URL: https://thecyphere.com/blog/nis2-penetration-testing/, accessed: 12.06.2025.

[11] Criminal code of Ukraine: Code of Ukraine of 05.04.2001 no. 2341-iii, 2001. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text, as of 7 June 2025. Accessed: 12.06.2025.

[12] On information: Law of Ukraine of 02.10.1992 no. 2657-xii, 1992. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text, as of 15 November 2024. Accessed: 12.06.2025.

[13] On information protection in information and communication systems: Law of Ukraine of 05.07.1994 no. 80-94-vr, 1994. URL: https://zakon.rada.gov.ua/laws/, as of 20 April 2025. Accessed: 12.06.2025.

[14] On the basic principles of cybersecurity in Ukraine: Law of Ukraine of 05.10.2017 no. 2163-viii, 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text, as of 20 April 2025. Accessed: 12.06.2025.

[15] B. Smith, Laws and regulations for penetration testing, LinkedIn, 2025. URL: https://www.linkedin.com/pulse/laws-regulations-penetration-testing-brian-smith-mlfpe/, accessed: 12.06.2025.

[16] Directive (EU) 2022/2555 of the European Parliament and of the council of 14 december 2022 on measures for a high common level of cybersecurity across the union, EUR-Lex, 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng, accessed: 12.06.2025.