DOI https://doi.org/10.32353/acfs.9.2024.06
UDC 343.1 (477)

Nataliia Filipenko,
Doctor of Law, Professor, Professor of the Law Department of National Aerospace University of National Aerospace University – "Kharkiv Aviation Institute" NAU "KhAI", Ukraine
ORCID: https://orcid.org/0000-0001-9469-3650
e-mail: n.filipenko@khai.edu

Anastasiia Kupriianova,
Deputy Director - Head of the department at National Scientific Center
«Hon. Prof. M. S. Bokarius Forensic Science Institute», PhD of law, Kharkiv, Ukraine
e-mail: anastasiya.k_ust@ukr.net

Aleksandar Ivanović,
Doctor of Law, Professor,
Director of Forensic Center Montenegro
Danilovgrad, Montenegro

Nataliia Filipenko

Anastasiia Kupriianova

Aleksandar Ivanović

Application Of Artificial Intelligence And Information And Communication Technologies In Prevention Of Cyberattacks On Critical Infrastructure Facilities

The article attempts to scientifically analyze certain aspects of unlawful (terrorist) influence on critical infrastructure and life support facilities in Ukraine. This research relevance is due to the real need to improve measures to counter cyber-terrorist attacks using the capabilities of artificial intelligence and information and communication technologies in order to create effective scientific and practical methods.

Keywords: *cyberspace, global Internet, terrorism, computer attacks, security, artificial intelligence, information technology, critical infrastructure, computer information.*

Introduction. The current global trend is convergence of socio-humanitarian and technical branches of knowledge. Modern technologies gradually and rapidly penetrate into various fields of human life. Law enforcement is no exception. Information and communication technologies are the subject of the study of forensic technology, but at the same time they can be a source of improvement of all branches of modern forensic science. Among the most promising and relevant of them is a group of related technologies, collectively referred to as artificial intelligence.

Artificial intelligence technologies are increasingly influencing various spheres of public life, determining not only the level of opportunities but the protection degree of social values[1].

According to provisions of the Development Concept of Artificial Intelligence in Ukraine, implementation of information technologies, which artificial intelligence technologies are a part is an integral component of development of socio-economic, scientific-technical, defense, legal and other activities in the fields of national significance. The lack of conceptual foundations of State policy in the field of artificial intelligence does not allow creating

[1] Філіпенко Н. Є., Лукашевич С. Ю. (2023). Інформаційні методики дослідження кримінальних правопорушень, вчинених з використанням технологій штучного інтелекту. *Наукові перспективи* (Серія «Державне управління», Серія «Право», Серія «Економіка», Серія «Медицина», Серія «Педагогіка», Серія «Психологія») Випуск № 11(41). 2023. Київ. 2023. № 1(7) С.1084-1096.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Disclaimer

The funder had no role in the study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Contributors

The author contributed solely to the intellectual discussion underlying this paper, case-law exploration, writing and editing, and accept responsibility for the content and interpretation.

Declaration of Competing Interest

The author declare that they have no conflict of interest.

and developing a competitive environment in the specified activity fields. The above indicates the need to develop a unified coordinated State policy aimed at solving various priority problems, including increasing the level of public safety through the use of artificial intelligence technologies during development of measures for the resocialization of convicted persons and the risk of reoffending[2]. The document states that main task of state policy in the field of legal regulation of the field of artificial intelligence is to ensure the protection of the rights and freedoms of participants in relations in the field of artificial intelligence...[3]

Every week, networks seem to grow in size and complexity. New SaaS services come online, while innovative communication tools make remote working easier. Data storage methods shift, with new assets to secure. And new malware threats constantly emerge. In an ever-changing digital world, network security has never been more crucial. Network security is not a fixed constant. Methods to protect networks change all the time[4].

With constant expansion and emergence of new digital opportunities, most countries in the world have strengthened cybersecurity measures. In this regard, new real and potential threats have emerged, the range of cyberattacks[5] on critical and socially significant infrastructure has expanded that requires ensuring sustainability of functioning of public and private corporate systems and networks.

With the massive increase in cyberattacks, recent reports show that hackers attack a computer in the US every 39 seconds[6]!

Thereby consideration of these issues, especially taking into account the sometimes-destructive influence of Russian hacker terrorist groups on the life of Ukrainian critical infrastructure facilities, is an urgent need and is of great relevance.

Literature Review. Some issues of the use of artificial intelligence and information and communication technologies in the prevention of cyber-terrorist attacks on critical infrastructure were considered by such scientists as Y Yu. M. Baturin, V. S. Venediktov V. V. Vertuzaiev, M. V. Viekhov, O. A. Havrylov, V. V. Holina, M. V. Karchevskyi, V. K. Kolpakov, O. V. Kokhanovska, S. Yu. Lukashevych, T. V. Mikhailina, M. I. Panov, V. V. Pyvovarov, M. S. Polievoi, V. A. Severyn, V. V. Sydorenko, K. S. Skoromnikov, H. O. Spitsyna, F. P. Tarasenko, L. K. Tereshchenko, T. I. Tarakhonych, B. S. Ukraintsev, N. Ye. Filipenko, V. S. Frolov, V. M. Shevchuk, V. Yu. Shepitko, A. V. Chernykh,

[2] Повідомлення про проведення публічного громадського обговорення проєкту розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку штучного інтелекту в Україні». Міністерство та комітет цифрової трансформації України : веб-сайт. URL: https:// thedigital.gov.ua/regulations/povidomlennya-pro-provedennya-publichnogogromadskogo-obgovorennya-proyektu-rozporyadzhennya-kabinetu-ministrivukrayini-pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini

[3] Там само.

[4] Network security basics. URL: https://nordlayer.com/learn/network-security/basics/

[5] Див. докладніше: Leblanc S.P., Partington A., Chapman I.M., Bernier M. An overview of cyber attack and computer network operations simulation. SpringSim (MMS), 2011, pp. 92–100.; Brown B., Cutts A., McGrath D., Nicol D.M., Smith T.P., Tofel B. Simulation of cyber-attacks with applications in homeland defense training. Sensors, and command, control, communications, and intelligence (c3i) technologies for homeland defense and law enforcement II. International Society for Optics and Photonics, 2003, Vol. 5071, pp. 63–71.; Kuhl M.E., Sudit M., Kistner J., Costantini K. Cyber-attack modeling and simulation for network security analysis. 2007 Winter Simulation Conference. IEEE, 2007, pp. 1180–1188.

[6] Cyber Training Center with Virtual Platform. URL: https://www.marshall.edu/cecs/cyber-training-center/

S. V. Yasechko and others. However, many theoretical and applied issues still remain debatable and require additional coverage and development, especially in the context of armed aggression of Russian Federation against Ukraine.

Aim. The aim of this article is to consider modern Ukrainian and foreign experience in countering the use of artificial intelligence and information and communication technologies in preventing cyber-terrorist attacks on critical infrastructure facilities in Ukraine.

Results and discussion. The most dangerous and destructive consequences are terrorist acts related to the use of weapons, ammunition or explosives, as they pose a real threat to people lives and health, cause destruction of industrial, economic or defense facilities. Investigation complexity of mentioned crimes is due to the following: rapid appearance of the latest developments in the field of weapons; weakness of the system for controlling movement of weapons and military supplies; manifestations of corruption, shortcomings of organizational and economic activity in the Armed Forces of Ukraine; large gaps in national-patriotic education of population; an increase in stress and psychological burden on society, emergence of panicky moods caused by existence of negative military, economic and social factors; activity of a large number of informal military-type associations; increase in social tendencies towards the resolution of conflicts by force, the spread of manifestations of cruelty and violence; low coordination of actions of law enforcement agencies during anti-terrorist operations; availability of a large database from open arrays of Internet on creation and use of weapons and explosive devices; availability of so-called "dual-use" means that can be used as components to create homemade weapons or explosive devices in free access; significant prevalence on the Internet of sites with overt extremist ideology, etc.[7]

Critical infrastructure facilities, which have the most devastating effect, were and will be particularly vulnerable to terrorist attacks. Program documents of the United Nations emphasize that "there remains a pressing need to redouble efforts and reaffirm commitments to the full promotion and protection of human rights and fundamental freedoms across all efforts to counter-terrorism and prevent violent extremism conducive to terrorism"[8].

Critical infrastructure facilities are attractive for a number of reasons. Firstly, they can be an attractive target because of their strategic value to society, especially in highly industrialized countries of the Western Hemisphere. Interfering with such facilities, ideally with ability to generate cascading effects, allows terrorists to maximize damage with just one shot and instill fear to levels that could not be achieved as easily by attacking "normal" targets. Secondly, they can be aimed at

[7] Спіцина Г. О., Філіпенко Н. Є. (2019) Терористична діяльність: кримінально-правова політика протидії // Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку : зб. тез доп. міжнар. наук.-практ. конф. до 25-річчя ХНУВС (18 квіт. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 189.

[8] UN Global Counter-Terrorism Strategy Special Rapporteur on counter-terrorism and human rights. URL: https://www.ohchr.org/en/special-procedures/sr-terrorism/un-global-counter-terrorism-strategy#:~:text=The%20UN%20Global%20Counter-Terrorism%20Strategy%20(A%2FRES%2F,States%27%20counter-terrorism%20priorities.

Наталія Філіпенко,
Анастасія Купріянова,
Олександр Іванович

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У ЗАПОБІГАННІ КІБЕРАТАКАМ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті зроблено спробу наукового аналізу окремих аспектів протиправного (терористичного) впливу на об'єкти критичної інфраструктури та життєзабезпечення в Україні. Така актуальність дослідження зумовлена реальною необхідністю вдосконалення заходів протидії кібертерористичним атакам з використанням можливостей штучного інтелекту та інформаційно-комунікаційних технологій з метою створення ефективних науково-практичних методів.

Ключові слова: кіберпростір, глобальна мережа Інтернет, тероризм, комп'ютерні атаки, безпека, штучний інтелект, інформаційні технології, критична інфраструктура, комп'ютерна інформація

Nataliia Filipenko,
Anastasiia Kupriianova,
Aleksandar Ivanović

ANWENDUNG KÜNSTLICHER INTELLIGENZ UND INFORMATIONS- UND KOMMUNIKATIONSTECH-NOLOGIEN ZUR VERHIN-DERUNG VON CYBER-ANGRIFF-EN AUF KRITISCHE INFRASTRUKTUROBJEKTE

Der Artikel versucht eine wissenschaftliche Analyse bestimmter Aspekte der illegalen (terroristischen) Einflussnahme auf Objekte kritischer Infrastruktur und Lebenserhaltung in der Ukraine. Diese Relevanz der Studie ist auf die tatsächliche Notwendigkeit zurückzuführen, die Gegenmaßnahmen gegen Cyberterrorangriffe mithilfe der Fähigkeiten künstlicher Intelligenz sowie Informations- und Kommunikationstechnologien zu verbessern, um wirksame wissenschaftliche und praktische Methoden zu schaffen.

Schlüsselwörter: Cyberspace, globales Netzwerk Internet, Terrorismus, Computerangriffe, Sicherheit, künstliche Intelligenz, Informationstechnologie, kritische Infrastruktur, Computerinformationen

demonstrating powerlessness of State institutions. For example, terrorist organizations may decide to attack energy facilities, oil pipelines, etc. to disrupt the supply of basic services and expose the fragility of government agencies and related government policies, etc.[9].

In UN Global Counter-Terrorism Strategy, under Chapter II: Measures to Combat and Prevent Terrorism, Member States decided to "intensify all efforts to increase security and protection of particularly vulnerable objects, such as infrastructure and public places, as well as the response to terrorist attacks and other disasters, particularly in the field of civil defense, while recognizing that States may need assistance for this purpose".

Security Council Resolution 1373 (2001) has already called on member states to "take the necessary measures to counter the commission of terrorist acts, including through early action to counter the commission of terrorist acts, including through early warning to other States through the exchange of information". Security Council resolution 1566 (2004) calls on states to prevent criminal acts, in particular against civilians, that are committed with the aim of inciting state of terror among population or a group of persons, intimidating population, or forcing a government or an international organization to commit or refrain from any what actions Physical protection of critical infrastructure facilities can prevent serious terrorist attacks. Moreover, immediate response to a terrorist attack on critical infrastructure can prevent cascading effects that are often associated with such attacks[10].

Resolution 1373 also obliges the Anti-Terrorism Task Force (ATTF) within the Office of Counter-Terrorism (OCT), Working Group on Critical Infrastructure Protection, including Vulnerable Critical Infrastructure Protection Targets, to continue working together on assistance in providing technical assistance and capacity building, as well as raising awareness in the field of protecting critical infrastructure objects from terrorist attacks, in particular by: strengthening dialogue with states, international and regional organizations (IROs) and working with technical assistance providers, in particular through the exchange of information[11].

Thereby, on February 17, 2017, Security Council of United Nations unanimously adopted resolution № 2341 on protection of critical infrastructure facilities and the expansion of capabilities of States to prevent attacks on critical infrastructure facilities and called on member states to confront the danger of terrorist attacks on them In the UN Global Counter-Terrorism Strategy, under Chapter II Measures to Combat and

[9] Акерман 2007, Оцінка мотивації терористів для нападу на критично важливі інфраструктури, Центр досліджень з нерозповсюдження, Монтерейський інститут міжнародних досліджень. URL: https://e-reports-ext.llnl.gov/pdf/341566.pdf

[10] Захист критично важливих об'єктів інфраструктури від терористичних атак: збірник передового досвіду. Контртерористичне управління Організації Об'єднаних Націй (КТУ ООН). Виконавчий директорат Контртерористичного комітету Ради Безпеки ООН (ИДКТК). 2018. URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf

[11] Захист критично важливих об'єктів інфраструктури від терористичних атак: збірник передового досвіду. Контртерористичне управління Організації Об'єднаних Націй (КТУ ООН). Виконавчий директорат Контртерористичного комітету Ради Безпеки ООН (ИДКТК). 2018. URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf , С. 5.

Prevent Terrorism, Member States decided to intensify all efforts to increase security and protection of particularly vulnerable objects, such as infrastructure and public places, and to respond to terrorist attacks and other disasters, particularly in the field of civil defense, recognizing that States may need assistance for this purpose[12].

Obviously, Researches on use of artificial intelligence and information and communication technologies in the prevention of cyber-terrorist attacks on critical infrastructure facilities is urgent task of modern science.

Currently, resources of information and telecommunication systems and networks largely ensure functioning and development of most areas of human activity. In addition, technical progress determines the transfer of interaction of individuals into digital space, according to which all material traces reflecting their communication, in order to ensure their procedural fixation, require detection, extraction and research of digital information.

Law of Ukraine: On the Basic Principles of Cybersecurity in Ukraine № 2163-VIII dated on October 5, 2017 defines protection of the vital interests of a person and citizen, society and the state during the use of cyberspace, when the sustainable development of the information society and digital communication environment is ensured, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace. In order to implement this law, Project of Cybersecurity Strategy Implementation of Ukraine will be implemented from 2022[13], providing for development of system of cyber security indicators, effective cyber defense, creation of units with authority to conduct armed conflict in cyberspace, effective countermeasures against intelligence and subversive activities in cyberspace and cyberterrorism, strengthening of technological and human resources potential of law enforcement agencies for prevention and investigation of cybercrimes, ensuring security of digital services and other important areas.

Wide distribution of digital communication leads to emergence of new ways of committing cyber-terrorist attacks on critical infrastructure facilities, mechanisms for creation and functioning of organized terrorist groups, complicating forms and methods of their criminal activities.

Cyber threats vary, but can include, for example, attacks that: manipulate systems or data such as malware that exploits vulnerabilities in the software and hardware components of computers needed to operate critical infrastructure or life support; disable critical systems, such as denial-of-service attack; restrict access to critical systems or information; for example, through ransomware attacks, introduction of malicious software through removable media and external equipment, etc.

APT attacks (Advanced Persistent Threat) are considered the most dangerous among such attacks. APT attacks are targeted cyber-attacks on the computer networks of a competitor (organization, state) using latent (those that are not

Nataliia Filipenko, Anastasiia Kupriianova, Aleksandar Ivanović

APPLICATION DE L'INTELLIGENCE ARTIFICIELLE ET DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION POUR PRÉVENIR LES CYBER-ATTAQUES SUR DES OBJETS D'INFRASTRUCTURE CRITIQUES

L'article tente une analyse scientifique de certains aspects de l'influence illégale (terroriste) sur les infrastructures critiques et les moyens de survie en Ukraine. Une telle pertinence de l'étude est due à la nécessité réelle d'améliorer les mesures contre les attaques cyberterroristes en utilisant les capacités de l'intelligence artificielle et des technologies de l'information et de la communication afin de créer des méthodes scientifiques et pratiques efficaces.

Mots-clés : cyberespace, réseau mondial Internet, terrorisme, attaques informatiques, sécurité, intelligence artificielle, technologies de l'information, infrastructures critiques, information informatique

[12] Захист критично важливих об'єктів інфраструктури від терористичних атак: збірник передового досвіду. Контртерористичне управління Організації Об'єднаних Націй (КТУ ООН). Виконавчий директорат Контртерористичного комітету Ради Безпеки ООН (ИДКТК). 2018. URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf

[13] План реалізації Стратегії кібербезпеки України Введено в дію Указом Президента України від 1 лютого 2022 р. № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

**Nataliia Filipenko,
Anastasiia Kupriianova,
Aleksandar Ivanović**

ZASTOSOWANIE SZTUCZNEJ INTELIGENCJI ORAZ TECHNOLOGII INFORMACYJNO-KOMUNIKACYJNYCH W PRZECIWDZIAŁANIU CYBERATAKOM NA KRYTYCZNE OBIEKTÓW INFRASTRUKTURY

W artykule podjęto próbę naukowej analizy niektórych aspektów nielegalnego (terrorystycznego) wpływu na obiekty infrastruktury krytycznej i systemów podtrzymywania życia na Ukrainie. Taka trafność badania wynika z realnej potrzeby doskonalenia środków przeciwdziałania atakom cyberterrorystycznym z wykorzystaniem możliwości sztucznej inteligencji oraz technologii informacyjno-komunikacyjnych w celu stworzenia skutecznych metod naukowych i praktycznych.

Słowa kluczowe: cyberprzestrzeń, globalna sieć Internet, terroryzm, ataki komputerowe, bezpieczeństwo, sztuczna inteligencja, technologie informacyjne, infrastruktura krytyczna, informacja komputerowa

outwardly visible) vulnerabilities in combination with covert intelligence or subversive actions. Their main purpose is to obtain, violate integrity or block information important for another State.

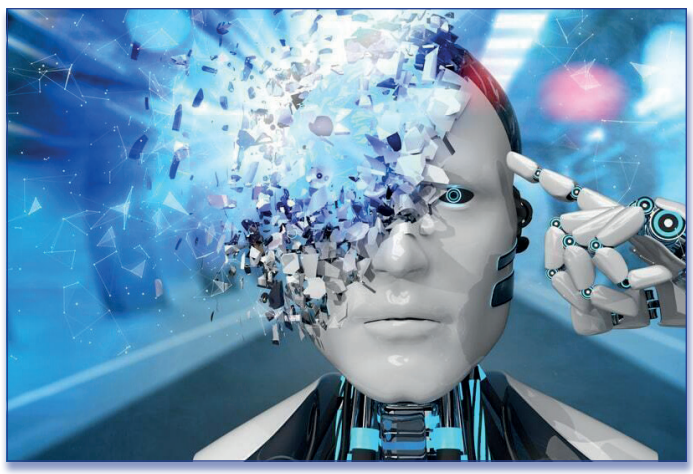
The main characteristics of APT attacks: cannot involve direct financial benefit, despite significant costs for their organization and implementation; are carried out by a group of highly qualified "hackers" according to the single project of leadership of special service; are carefully disguised using specially developed software tools (special shell-codes, rootkits, 0-day vulnerabilities, etc.); use latent vulnerabilities that remain unknown for a long time and are not detected by any antiviruses; supported by reconnaissance or subversive actions or are elements of these actions.

Data on a series of cyberattacks that took place in Ukraine and were directed primarily against objects of critical infrastructure of our state were published at the Virus Bulletin conference and within the framework of the Cisco Cybersecurity Technologies forum (December 8, 2016). Among the number of known methods of initiating information security incidents, the undisputed leader is the infection of users with malicious software (70.2%). In 2016, attackers mainly used the 0day attack for this purpose. It is followed by spam, phishing and various types of Internet fraud (52.5%), DoS attacks (37.4%), spyware attacks (20%), ransomware (18.5%), targeted hacker attacks (15.1%) and botnets (12.5%).

The problem of using capabilities of artificial intelligence to commit cyber-terrorist attacks on critical infrastructure facilities is currently relevant. It is used to find vulnerabilities and implement phishing attacks, bypass biometrics and create fake profiles in social networks, etc. (for example, creating fake master fingerprints, spoofing faces in video images, etc.).

A pressing problem is the use of 5G networks as a platform for cyber-terrorist attacks, because the use of this technology will significantly increase the power of DDoS attacks.

In this context, reliable and accurate short-term forecasts of non-state terrorism at the local level are key for policymakers to target preventive measures. As scientist note researches on armed conflict and insurgency has led to development of theory-based[14] predictive models including successful research program applying artificial intelligence capabilities to predict conflict at a precise space temporal scale[15]. However, this important information obtained from research on armed conflicts has not yet found its way into research on terrorism. Terrorism research has generally focused on explanatory models using statistical approaches to capture and quantify the effects of the driving forces of terrorist attacks across space and time16. Thus, there is a need to develop an interpretable simulation model for predicting terrorist events at precise spatial and temporal scales that can



[14] M. Lim, R. Metzler, Y. Bar-Yam (2007) Global pattern formation and ethnic/cultural violence. Science. P. 1540–1544.; A. Zammit-Mangion, M. Dewar, V. Kadirkamanathan, G. Sanguinetti (2012) Point process modelling of the Afghan War Diary. Proc. Natl. Acad. Sci. U.S.A. 109, 12414–12419.

[15] H. Hegre, J. Karlsen, H. M. Nygard, H. Strand, H. Urdal (2013) Predicting armed conflict, 2010–2050. Int. Stud. P. 250–270. P.50.

[16] S. C. Nemeth, J. A. Mauslein, C. Stapley (2014) The primacy of the local: Identifying terrorist hot spots using geographic information systems. J. Polit. P. 304–317.

help implement effective interventions and evaluate and develop theories at appropriate scales[17].

Dr. Andre Python from Zhejiang University (China) and colleagues found a way to improve the work of artificial intelligence in this area. Researches developed a framework for predicting terrorist attacks around the world by first examining terrorist attacks that occurred between 2002 and 2016 (i.e., during 795 weeks) in 13 regions including all subcontinental regions listed in the Global Terrorism Database (GTD) and West Africa. For each region, predictive models were built that allow identifying, evaluating and comparing the role of the main driving forces of terrorism. The researchers developed interpretable tree-based machine learning algorithm with so-called gradient boosting. In order to capture all regions of the world potentially affected by terrorism over a long period of time, the authors divided the regions into cells, each covering an area of 50 × 50 km, and set a time parameter of 795 weeks. Next, the work included a tree-like machine learning algorithm that analyzed probability of terrorist attacks (and retaliatory measures) in each cell every week around the world[18].

According to scientists, machine algorithms are quite effective in predicting events in areas that have been repeatedly attacked, but it is difficult for them to build forecasts for regions where there have been no terrorist attacks for a long time. This data imbalance reduces accuracy of models, but it can be achieved by applying additional parameters[19].

Scientists have identified two main goals of terrorism: intimidation and provocation. In the first case, the terrorists try to force them to comply with their demands, and in the second, they try to force them to counterattack with them. In both cases, they use violence as communication.

Researchers identified 6 main variables that increase possibility of terrorist attacks:

– proximity to the capital, large cities and roads for faster dissemination of the message.

– geographical advantage of terrorists; they often hide in hard-to-reach places and can choose targets for intimidation closer to their base.

– economic activity of the region; the more developed the country, the more damage a terrorist attack can cause.

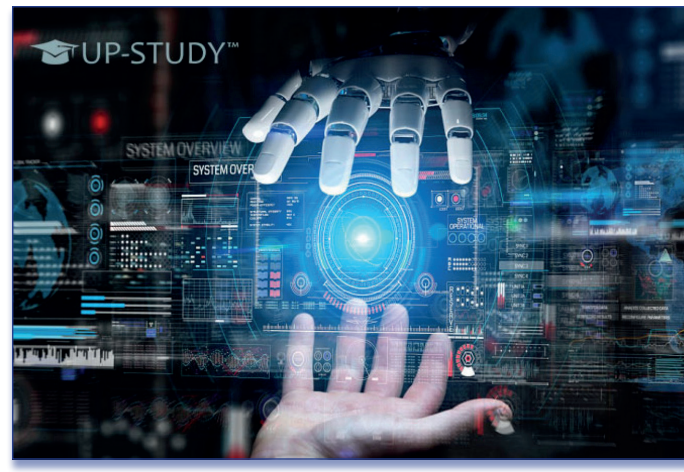
– likelihood of conflict escalation terrorists regularly tries to unleash local wars in order to recruit new followers.

– political regime and GDP indicator: level of democracy affects the choice of strategy of action by terrorists.

[17] Andre Python, Andreas Bender, Anita K. Nandi, Penelope A. Hancock, Rohan Arambepola, Jürgen Brandsch and Tim C. D. Lucas (2021) Predicting non-state terrorism worldwide. URL: https://www.science.org/doi/10.1126/sciadv.abg4778

[18] Комп'ютер проти тероризму: вчені навчили ШІ передбачати теракти по всьому світу. URL: https://focus.ua/uk/digital/489637-kompyuter-protiv-terrorizma-uchenye-nauchili-ii-predskazyvat-terakty-po-vsemu-miru.

[19] Губарєв І., Харченко В. Використання можливостей штучного інтелекту для попередження терористичних атак на об'єкти критичної інфраструктури. Безпека та сталий розвиток критичної інфраструктури в умовах воєнного стану [Електронний ресурс] : тези доповідей науково-практичної конференції, 8 листопада 2023 р., Харків / Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут». Харків : ХАІ, 2023. С. 44-48. URL: https://dspace.library.khai.edu/xmlui/bitstream/handle/123456789/5878/Bezpeka_ta_stalyy_rozvytok.pdf?sequence=4&isAllowed=y



– local consolidation: likelihood of a recurrence of terrorist attacks largely depends on whether the organization was able to create cells in a particular region20.

Conclusions. Taking into account the above, we consider it necessary to propose the following ways to counteract cyber-terrorist attacks on critical infrastructure facilities, namely:

1. Develop risk profiles for specific critical infrastructure sectors. These profiles are critical to assessing existing mitigation practices, outcomes, and vulnerabilities. Depending on the sector considered, risk assessments can be carried out for specific facilities. For example, Australia Critical Infrastructure Resilience Strategy breaks down the transport sector into the following subsectors: aviation, land passenger transport (including bridges and tunnels), land transport and sea transport (shipping and ports). In accordance with the same strategy, energy sector consists of electricity supply systems, offshore oil and gas fields, onshore oil and gas and coal supplies.

2. Create cards for organization of cyber defense of critical infrastructure facilities. Such a card contains key elements of cyberattacks on critical infrastructure and offers options for protecting them from possible actions of cybercriminals. At the same time, any cyberattack according to the map can be presented in the form of a certain algorithm of actions, which use will significantly reduce the time for organizing cyber defense and increase effectiveness of the decisions made.

3. Launching cyber training grounds and conducting command and staff exercises with the involvement of a wide range of interested specialists from both the public and private sectors. A vivid example of this can be the activity of the Air Force Cyber Command (AFCYBER), one of the main commands of the US Air Force. Based at Barksdale Air Force Base. Just as the aviation and space units are called upon to conduct reconnaissance, defense and offensive operations in airspace and outer space, cyber unit is responsible for cyberspace. According to Secretary of Defense Michael Wynn, the need to create a military cyber unit is caused by intensification of activities of foreign hackers against United States[21]. Tasks and functions of the unit: conducting defensive and offensive operations related to intrusion into IT systems of a potential adversary; protection of information and technical systems of American military, as well as critical nodes of American Internet; studying hardware bookmarks and vulnerabilities that can be remotely used to disable military systems, or remove data from them, etc.

A successful Ukrainian example can be considered the launch of the Unit Range cyber training ground, which was created for the practical training of cyber security specialists in conditions as close as possible to real ones. This was reported by Yehor Aushev, the founder of the training ground and expert in cyber security. There are already more than 150 scenarios in the system, and specialists from Ukrainian state bodies are trained. Unit Range was created directly during the war, and its developers took into account the features of modern warfare, where combat operations are often combined with cyberattacks and attempts to destroy the enemy digital infrastructure. In addition, Unit Range provides a real-time data dashboard that measures performance and risk profile of all team members, from executives to regular IT staff[22].

4. Special technological solutions are being developed to prevent mass terrorist attacks, riots, and ensure security at mass events. For example, the

[20] Комп'ютер проти тероризму: вчені навчили ШІ передбачати теракти по всьому світу. URL: https://focus.ua/uk/digital/489637-kompyuter-protiv-terrorizma-uchenye-nauchili-ii-predskazyvat-terakty-po-vsemu-miru.

[21] Кібернетичне командування Повітряних сил США. URL: https://uk.wikipedia.org/wiki/Кібернетичне_командування_Повітряних_сил_США

[22] Єгор Аушев запустив кіберполігон для тренування спеціалістів — там вже є понад 150 сценаріїв атаки і захисту. URL: https://dou.ua/lenta/news/about-unit-range/

Evolv Technology company has developed a security machine based on artificial intelligence, which works through the Evolv Pinpoint application and uses of facial recognition feature. The structure can be installed at the entrance to commercial establishments, schools, shopping centers, airports, night clubs, restaurants, etc. To check, it is enough for a person to go through the structure as through a regular metal detector. The throughput of such detector is 600-900 people per hour. The check is carried out by a built-in camera, Evolv Pinpoint algorithms match the visitors' faces with people on the watch list loaded into the system database. If it turns out that the visitor is of interest to the police or other services, his image and personal data are displayed on the security officer's tablet, highlighted in red. Yellow lighting indicates an unverified threat. The profile is then verified in real time within seconds[23].

5. Extensive cooperation of State, commercial and public structures in the development of conceptual principles and recommendations for countering cyber-terrorist attacks on critical infrastructure facilities.

References:

Andre Python, Andreas Bender, Anita K. Nandi, Penelope A. Hancock, Rohan Arambepola, Jürgen Brandsch and Tim C. D. Lucas (2021) Predicting non-state terrorism worldwide. URL: https://www.science.org/doi/10.1126/sciadv.abg4778 [in English].

Brown B., Cutts A., McGrath D., Nicol D.M., Smith T.P., Tofel B. (2003) Simulation of cyber-attacks with applications in homeland defense training. Sensors, and command, control, communications, and intelligence (c3i) technologies for homeland defense and law enforcement II. International Society for Optics and Photonics, Vol. 5071, Pp. 63–71. [in English].

Cyber Training Center with Virtual Platform. URL: https://www.marshall.edu/cecs/cyber-training-center/ [in English].

Hegre H., Karlsen J., H. M. Nygård, H. Strand, H. Urdal (2013) Predicting armed conflict, 2010–2050. Int. Stud. P. 250–270. [in English].

Kuhl M.E., Sudit M., Kistner J., Costantini K. (2007) Cyber-attack modeling and simulation for network security analysis. 2007 Winter Simulation Conference. IEEE, Pp. 1180–1188. [in English].

Leblanc S.P., Partington A., Chapman I.M., Bernier M. (2011) An overview of cyber attack and computer network operations simulation. SpringSim (MMS), Pp. 92–100. [in English].

Lim M., Metzler R., Bar-Yam Y. (2007) Global pattern formation and ethnic/cultural violence. Science. Pp. 1540–1544. [in English].

Nemeth S. C., Mauslein J. A., Stapley C. (2014) The primacy of the local: Identifying terrorist hot spots using geographic information systems. J. Polit. Pp. 304–317. [in English].

Network security basics. URL: https://nordlayer.com/learn/network-security/basics/

UN Global Counter-Terrorism Strategy Special Rapporteur on counter-terrorism and human rights. URL: https://www.ohchr.org/en/special-procedures/sr-terrorism/un-global-counter-terrorism-strategy#:~:text=The%20UN%20Global%20Counter-Terrorism%20Strategy%20(A%2FRES%2F,States%27%20counter-terrorism%20priorities. [in English].

Zammit-Mangion A., Dewar M., Kadirkamanathan V., Sanguinetti G. (2012) Point process modelling of the Afghan War Diary. Proc. Natl. Acad. Sci. U.S.A. 109, Pp. 12414–12419. [in English].

Akerman 2007, Otsinka motyvatsiyi terorystiv dlya napadu na krytychno vazhlyvi infrastruktury, Tsentr doslidzhen' z nerozpovsyudzhennya, Montereys'kyy instytut mizhnarodnykh doslidzhen'. URL: https://e-reports-ext.llnl.gov/pdf/341566.pdf 1 [in Ukrainian].

Amerykans'kyy startap tayemno vyprobuvav systemu peredbachennya zlochyniv. URL: https://techno.nv.ua/ukr/innovations/velikij-brat-amerikanskij-startap-tajemno-viprobuvav-u-novomu-orleani-sistemu-peredbachennja-zlochiniv-2455319.html [in Ukrainian].

[23] Американський стартап таємно випробував систему передбачення злочинів. URL: https://techno.nv.ua/ukr/innovations/velikij-brat-amerikanskij-startap-tajemno-viprobuvav-u-novomu-orleani-sistemu-peredbachennja-zlochiniv-2455319.html

Gubarev I., Kharchenko V. (2023) Use of artificial intelligence capabilities to prevent terrorist attacks on critical infrastructure facilities. Security and sustainable development of critical infrastructure in the conditions of martial law [Electronic resource]: theses of reports of the scientific and practical conference, November 8, 2023, Kharkiv / Ministry of Education and Science of Ukraine, National Aerospace University named after M.E. Zhukovsky "Kharkiv Aviation Institute". Kharkiv: KHAI, Pp. 44-48. URL: https://dspace.library.khai.edu/xmlui/bitstream/handle/123456789/5878/Bezpeka_ta_stalyy_rozvytok.pdf?sequence=4&isAllowed=y [in Ukrainian].

Yehor Aushev zapustyv kiberpolihon dlya trenuvannya spetsialistiv — tam vzhe ye ponad 150 stsenariyiv ataky i zakhystu. URL: https://dou.ua/lenta/news/about-unit-range/ [in Ukrainian].

Zakhyst krytychno vazhlyvykh ob'yektiv infrastruktury vid terorystychnykh atak: zbirnyk peredovoho dosvidu. Kontrterorystychne upravlinnya Orhanizatsiyi Ob'yednanykh Natsiy (KTU OON). Vykonavchyy dyrektorat Kontrterorystychnoho komitetu Rady Bezpeky OON (YDKTK). 2018. URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf [in Ukrainian].

Kibernetychne komanduvannya Povitryanykh syl SSHA. URL: https://uk.wikipedia.org/wiki/Кібернетичне_командування_Повітряних_сил_США [in Ukrainian].

Komp'yuter proty teroryzmu: vcheni navchyly SHI peredbachaty terakty po vs'omu svitu. URL: https://focus.ua/uk/digital/489637-kompyuter-protiv-terrorizma-uchenye-nauchili-ii-predskazyvat-terakty-po-vsemu-miru [in Ukrainian].

Plan realizatsiyi Stratehiyi kiberbezpeky Ukrayiny Vvedeno v diyu Ukazom Prezydenta Ukrayiny vid 1 lyutoho 2022 r. № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text [in Ukrainian].

Povidomlennya pro provedennya publichnoho hromads'koho obhovorennya proyektu rozporyadzhennya Kabinetu Ministriv Ukrayiny «Pro skhvalennya Kontseptsiyi rozvytku shtuchnoho intelektu v Ukrayini». Ministerstvo ta komitet tsyfrovoyi transformatsiyi Ukrayiny : veb-sayt. URL: https:// thedigital.gov.ua/regulations/povidomlennya-pro-provedennya-publichnogogromadskogo-obgovorennya-proyektu-rozporyadzhennya-kabinetu-ministrivukrayini-pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini [in Ukrainian].

Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny. Zakon Ukrayiny vid 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

Spitsyna H. O., Filipenko N. YE. (2019) Terorystychna diyal'nist': kryminal'no-pravova polityka protydiyi // Kryminal'no-pravovi ta kryminolohichni zasoby protydiyi zlochynam proty hromads'koyi bezpeky ta publichnoho poryadku : zb. tez dop. mizhnar. nauk.-prakt. konf. do 25-richchya KHNUVS (18 kvit. 2019 r., m. Kharkiv) / MVS Ukrayiny, Kharkiv. nats. un-t vnutr. sprav; Kryminol. asots. Ukrayiny. Kharkiv : KHNUVS. Pp. 188-191. [in Ukrainian].

Filipenko N.YE., Lukashevych S.YU. (2023) Informatsiyni metodyky doslidzhennya kryminal'nykh pravoporushen', vchynenykh z vykorystannyam tekhnolohiy shtuchnoho intelektu. Naukovi perspektyvy (Seriya «Derzhavne upravlinnya», Seriya «Pravo», Seriya «Ekonomika», Seriya «Medytsyna», Seriya «Pedahohika», Seriya «Psykholohiya») Vypusk № 11(41)2023. Kyiv. 2023. № 1(7) C.1084-1096. [in Ukrainian].

Received by Editorial Board: 26.02.2024

Suggested Citation:

Filipenko, N., Kupriianova, A., Ivanovych, O. (2024). Application Of Artificial Intelligence And Information And Communication Technologies In Preventing Cyber Attacks On Critical Infrastructure Objects. *Archives of Criminology and Forensic Sciences*. 1 (9). 87-96. DOI: https://doi.org/10.32353/acfs.9.2024.06