Analysis of the Use of Information Resources of the Aggressor Country by the University Educational Process Participants in 2021-2023

Dmytro Tarasov and Maria Komova

Lviv Polytechnic National University, Stepana Bandery Srt. 12, Lviv, 79013, Ukraine

Abstract

An analysis of the activity of the use of the aggressor country's information resources by university educational process participants in 2021-2023 was carried out. Changes in the use of various resources before and after Russia's large-scale military attack on Ukraine are determined. Threats of using Russian information resources and data exchange systems are analyzed using Telegram as an example.

Keywords

website traffic analysis, traffic sources, Russian aggression, traffic sources, referrals, information security, university E-Learning System, Telegram

1. Introduction

After Russia's large-scale military attack on Ukraine, which began on February 24, 2022, the technologies of Ukrainian users' work with Internet information resources and communication services have changed significantly.

The use of Russian news sites by users from Ukraine is decreasing, and the percentage of Ukrainian-language searches in search engines and youtube.com is increasing.

The purpose of the work is to investigate changes in the activity of using the information resources of the aggressor country (Russia) by teachers and students of the Lviv Polytechnic National University. The analysis of the use of Russian resources was carried out on the example of changes in the number of transitions (sessions) of visitors to the Virtual Learning Environment of the Lviv Polytechnic (VNS) [1, 9, 10] from other Internet resources.

2. Study of the activity of the use of various resources by the VNS users

2.1. General information about the sources of user transitions to the VNS website

University e-learning system is an open source learning management system, with a focus on development of the cooperation between university teachers and students. It is based on using the Moodle platform. Moodle [12, 13, 18] system has a wide selection of functionality commonly found in e-learning platforms, course management systems, learning management systems (LMS) or virtual learning environments (VLE). The basic Moodle's advantage is that this web service provides an opportunity to create efficient websites for online learning [5, 10, 21].

SCIA-2023: 2nd International Workshop on Social Communication and Information Activity in Digital Humanities, November 9, 2023, Lviv, Ukraine

EMAIL: dmytro.o.tarasov@lpnu.ua (D. Tarasov); mariia.v.komova@lpnu.ua (M. Komova)
ORCID: 0000-0002-7143-8558 (D. Tarasov); 0000-0002-4115-3690 (M. Komova)

The VNS system on the Moodle platform is actively used throughout the academic year 2021-2023. VNS (https://vns.lpnu.ua/) users are all teachers and students of the Lviv Polytechnic National University. The total number of VNS users exceeds 30,000.

Google Analytics was used to obtain information about visits to the VNS website, count the number of user sessions, and analyze the sources of transitions [14. 23]. Google Analytics statistics do not include traffic from robots, crawlers, and other technical traffic to the VNS website.

For comparison, the indicator of the share of the number of sessions [2, 11] to the total number of users' sessions and the change of these indicators during three periods was used:

1. "I semester". Academic year 2021/22 Fall semester (before the full-scale invasion of 2022). Sample behavior of VNS users before a full-scale intrusion.
2. "II semester". Corresponding autumn term academic year 2022/23 (6 months after the full-scale invasion of 2022).
3. "III semester". Spring Semester academic year 2022/23 (11 months after full-scale invasion).

For the convenience of analysis, the visitors' transitions sources were grouped into:

- direct transfer (or no established transfer source);
- browser hijackers (or search plugins);
- group work and communication tools;
- tools for education and performing (distribution) of assignments;
- translation tools;
- educational, scientific sites;
- portal ukr.net;
- email;
- search engines (except Russian);
- websites of the university and divisions;
- social networks;
- Russian Internet resources;
- resources controlled by Russia – the Telegram messenger;
- other sites.

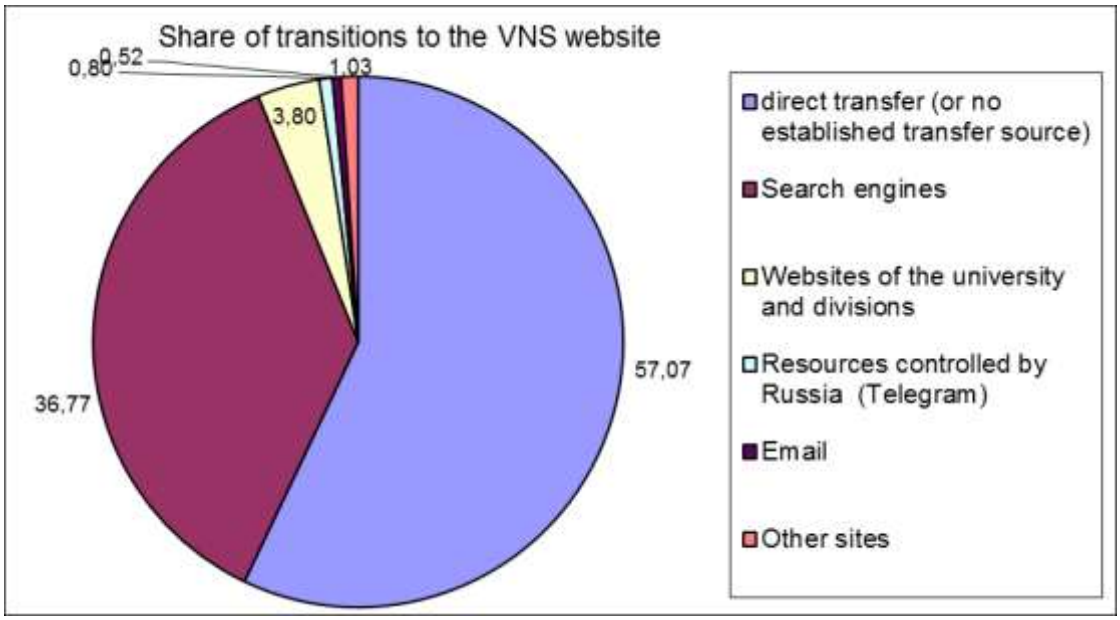

Figure 1: Share of transitions to the VNS website distribution. Popular sources for 3 semesters

For further analysis, it is important to determine the means of communication used by users and the information resources from which users go to VNS.

More than 57% of user transitions to the VNS website do not have information about the external source of the transition (references). Most of them are direct transitions or transitions with missing information about the source.

Other options for hiding information about the source of transitions are:

- determining that source is a Proxy address, VPN, browser manufacturer's site, local network address, etc.;
- identification that source is a Browser hijacker or it`s search engines;
- identification that source is a technical address related to cyber attacks.

The distribution of unknown and hidden sources is shown in Table 1.

Table 1

Various undefined transition sources (source types)

Source types	Transitions, %
Direct	57,07
Browser hijackers	0,12
Local network addresses	0,06
Short links	0,02
Cyberattack	0,02
Proxy, VPN, браузери	0,01
Total	57,30

2.2. Use of various sources by VNS users

Let's consider the sources of transitions to the VNS website from identified sites, means of communication (mail systems, messengers, social networks, etc.), and means of e-learning and group work.

The diagram (Fig. 2.) shows the shares of the number of VNS users sessions for which the transition sources were various sites during three semesters. Search engines, direct links, local network addresses, etc. are excluded from the data in Fig. 2.

More than 61% of the sessions in Fig. 2. started after the transition from university sites, more than 13% from the Telegram messenger controlled by Russian representatives, 8.67% from e-mail services, and 1.85% from Russian sites and systems excluding Telegram.

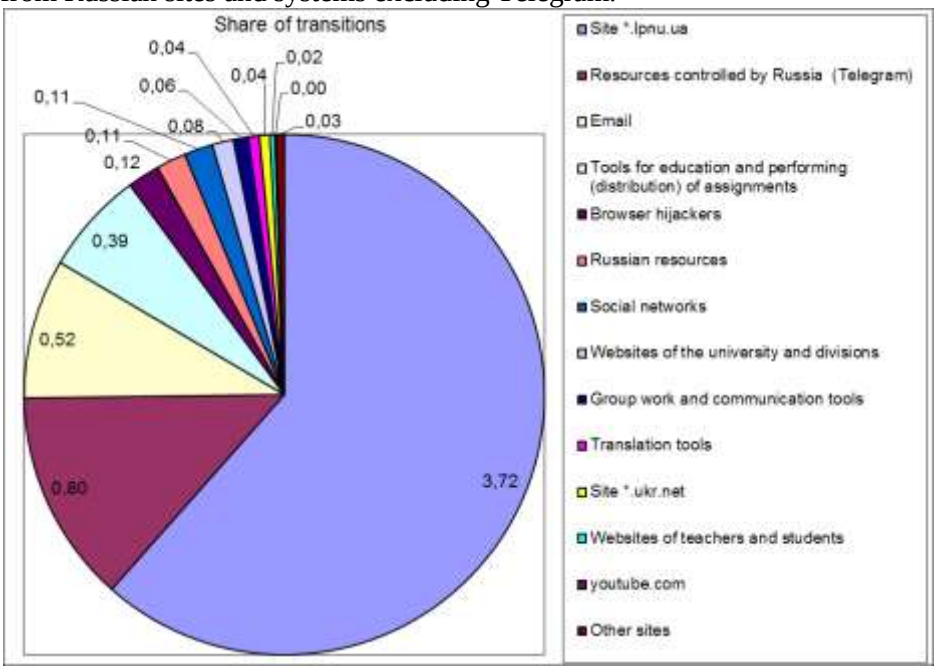

Figure 2: Distribution of the VNS visitors sessions quantity during selected semesters for known sources

Detailed information on the total share of transitions from different resource types is given in Table 2.

Table 2
Total share of transitions from different resource types

Source type	Transitions, %
Site *.lpnu.ua	3,72
Resources controlled by Russia (Telegram)	0,80
Email	0,52
Tools for education and performing (distribution) of assignments	0,39
Browser hijackers	0,12
Russian resources	0,11
Social networks	0,11
Websites of the library and university departments	0,08
Group work and communication tools	0,06
Translation tools	0,04
Site *.ukr.net	0,04
Websites of teachers and students	0,02
youtube.com	<0,01
Other sites	0,03
Total	6,04

The diagram (Fig. 3.) compares the number of sessions with defined user transitions during particular semesters of 2021-2023 (excluded transitions from the university website and university divisions).

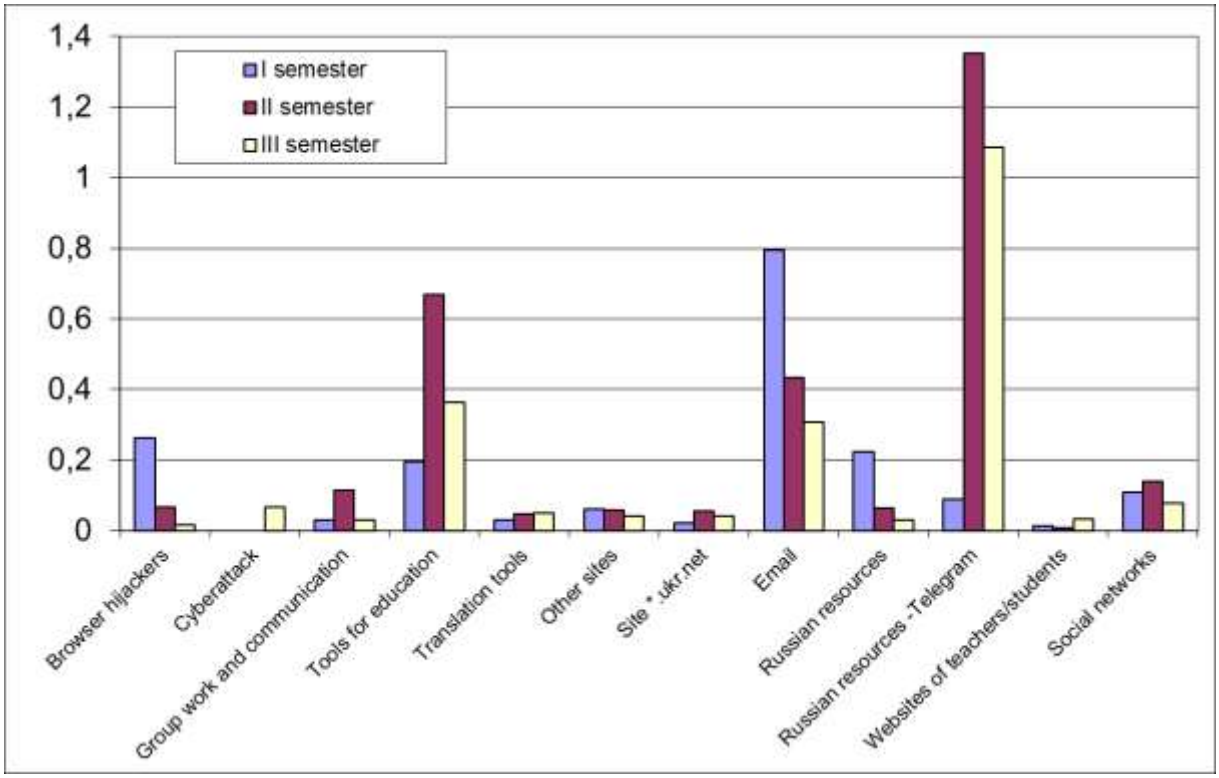

Figure 3: Shares of the sessions quantity with defined user transitions in particular semesters

Taking into account the transitions of the university website and university divisions, the dynamics of changes in the frequency of various transitions sources use over three semesters is presented in Table 3.

Table 3

The use of various transitions sources by VNS users

Source type	I semester	II semester	III semester
Site *.lpnu.ua	0,99	5,90	4,99
Browser hijackers	0,26	0,07	0,02
Cyberattack	0	0	0,07
Group work and communication tools	0,03	0,11	0,03
Tools for education and performing (distribution) of assignments	0,19	0,67	0,36
Translation tools	0,03	0,05	0,05
Other sites	0,06	0,06	0,04
Site *.ukr.net	0,02	0,06	0,04
Email	0,80	0,43	0,31
Russian resources	0,22	0,06	0,03
Russian resources - telegram	0,09	1,35	1,09
Websites of teachers/students	0,01	0,01	0,03
Social networks	0,11	0,14	0,08
Total	2,81	8,91	7,14

Among the popular resources of the type "Group work and communication tools" are instant messengers, tools for sharing files, notes, URLs, messages, etc. This section does not include known Russian resources. Examples of popular resources of the "Group work and communication tools":

- onenote
- skype
- trello
- keep google
- mindomo.com
- canva.com
- workona.com
- calendar.google.com
- getpocket.com
- wakelet.com

The popular resources of the type "Tools for education and performing (distribution) of assignments" include tools for video conferences, systems for conducting training, joint work with files (projects), and distribution of educational content, tests, etc. This section does not include known Russian resources. For example:

- Google classroom
- MS Teams
- Zoom
- youtube.com
- wps.com

- docs.google
- mubu.com
- feishu.cn
- wps.com

Resources of type "Translation tools" include Google Translate and it's tools embedded in websites.

Popular resources of the type "Email" include E-Mail servers. This section does not include known Russian resources. Example:

- Gmail
- QQ
- Ukr.net

The Ukr.net service is mainly used by VNS visitors as a popular email postal service in Ukraine. But *.ukr.net domain sites also provide access to file storage, news, etc.

Popular resources of the "Social networks" type include such international social networks as:

- instagram
- facebook
- twitter

Data in Fig. 3. and Table 3 demonstrate the change in the activity of using Internet services by users during the 3 semesters of 2021-2023:

- gradual reduction of transitions from e-mail (shares of transitions – 0.8; 0.43; 0.31);
- gradual reduction of conversions from tools such as browser hijackers (share of conversions – 0.26; 0.07; 0.02);
- a gradual reduction in conversions from Russian sites and systems except for Telegram (shares of conversions – 0.22; 0.06; 0.03);
- a significant increase in conversions from Telegram compared to the first semester (shares of conversions – 0.09; 1.35; 1.09);
- relative stability of the share of transitions from other classified sources, including social networks.

The largest redistribution of user traffic occurs due to the increase in transitions from university sites, and usage of Telegram and educational tools (Table 4).

Table 4

Sources with decreasing and increasing traffic for 2021-2023

Sources with a decreasing number of transitions	Difference, %	Difference, %	Sources with an increasing number of transitions
		4	Site *.lpnu.ua
Browser hijackers	-0,24		
Group work and communication tools	0		
		0,17	Tools for education and performing (distribution) of assignments
		0,02	Translation tools
		0,02	Site *.ukr.net
Email	-0,49		
Russian resources	-0,19		

		1	Resources controlled by Russia (Telegram)
		0,02	Websites of teachers and students
Social networks	-0,03		
Other sites	-0,02		
Total	-0,97	5,23	

3. Popular Russian resources and services are identified

While the usage of Russian sites in Ukraine is gradualy decreasing, the growth of Telegram use is a reason to concern about.

The following sources are attributed to Telegram resources in the received transition data:
transitions from mobile clients, desktop version of Telegram, and web version;
transitions from unofficial and alternative clients;
transitions from the telegra.ph blog platform developed for Telegram.

The following domains were used to identify transitions:

- “web.tlgrm.app”
- “web.telegram.org”
- “telegra.ph”
- “webz.telegram.org”
- “т.online”
- “телеграм.онлайн”
- “webogram.ru”

Other Russian sites and means of communication identified in the study include:

- Yandex search engine and portal resources (yandex search sites from UA, RU and other national domains);
- Yandex email system;
- Email and sites of the domain *.mail.ru;
- Site top-page.ru;
- Vkontakte social network (website vk.com).

The study also found a small number of transitions from other sites in the RU and SU domains.

4. Risks of using Telegram

The study found that Telegram is the most popular communication service for sharing links to educational materials among university students and teachers. Even university corporate services (Email and MS Teams) are not used as actively as Telegram for exchanging links to educational materials and VNS resources.

Telegram's popularity increased after the Russian attack in 2022. Unfortunately, this popularity is a general trend in Ukraine.

The Telegram owner and team are formally independent of the government and the Russian Federation and call themselves an independent international company. Researchers of Telegram's development history and financing point to Telegram's dependence on Russian funding. The studies also provide information on Telegram's possible cooperation with security organizations of the Russian Federation (Federal Security Service, FSB, Federal Service for Supervision of Communications, Information Technology and Mass Media, Roskomnadzor) [17. 19, 25].

Telegram provides additional means of authenticating users and obtaining their biometric and passport data [6].

Security components of cryptographic protection and the MTProto protocol are discussed in [3, 6]. Researchers consider custom-designed encryption protocol MTProto to be a theoretical vulnerability [16].

System problems with data security in Telegram are presented in works [7, 20,24].

General issues of personal data protection of Telegram users are considered in [2, 4, 15].

The problem for Ukraine is the spread of fake news and propaganda of violence against Ukrainians in Telegram. Since 2014, Telegram has been regularly accused of promoting propaganda and information manipulation, influencing Ukrainian politics [8, 26].

The set of technical problems with the security of the Telegram platform and the facts given in the literature about the concealment of Telegram's connections with the authorities of the aggressor country indicate a risk for users of the university and Ukraine.

The habit of using Telegram at the university further increases the risks for the personal data of university graduates and the possibility of their manipulation by the aggressor country.

5. Conclusions

Russia's major aggression against Ukraine in February 2022 caused systemic social and technical communication problems. Due to hostilities, forced migration, lack of electricity, and access to the Internet, university students and teachers have changed information sources (communication platforms). It is confirmed by change of the ways students access the educational materials (VNS website).

Analysis of the collected data shows the following trends after the full-scale invasion of Russia on February 24, 2022:

- a significant change in the popularity of means of communication and typical Internet services by users of the VNS;
- decrease of transitions from e-mail by 2.6 times (possibly due to competition with Telegram);
- growth in the use of educational tools by 2-3 times;
- growth of transitions from university sites by 6-6.2 times;
- a significant increase in the use of Telegram by 12-15 times;
- reduction of switching from other Russian services by 7.3 times.

Positive trends are an increase in the use of university resources, teachers, or specialized communication systems in which classes are held. Also, the good news is the decrease in the use of Russian sites and services as search engines and means of exchanging links or information.

A negative trend is a significant increase in the use of Telegram services in Ukraine and the educational environment. The Telegram platform is considered as system with significant risks for user information and flaws in encryption algorithms. Telegram is also accused of having ties with the authorities of the aggressor country and concealing funding.

6. References

[1] A. Andrukhiv, D. Tarasov, M. Sokil, The system of information providing of educational process in university, in: Proceedings of the 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Lviv, Ukraine, 2016, pp. 828-830, doi: 10.1109/TCSET.2016.7452197.

[2] A. Peleschyshyn, R. Korzh, O. Trach, M. Tsiutsiura, Building of Information Activity Management System of Higher Educational Establishment in the Social Environments of the Internet, in; 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019, pp. 58-61.

[3] B. Cogliati, J. Ethan, A. Jha, Subverting Telegram’s End-to-End Encryption, ToSC 1 (2023) 5–40.

[4] C. Bogos, R. Mocanu, E. Simion, A security analysis comparison between Signal, WhatsApp and Telegram, Cryptology ePrint Archive, 2023, URL: https://eprint.iacr.org/2023/071.

[5] C. Rodríguez, R. Rodríguez, G. Moure, C. L. Pérez, Personalization of Moodle with the integration of most used Web technologies in higher education, ITECKNE 16(1) (2019).
[6] D. Canellis, Telegram Passport is already drawing fire for not being secure enough, 2018. URL: https://thenextweb.com/news/telegram-passport-passwords-crack.
[7] D. Manish, Telegram, stop calling Cloud Chats encrypted, let alone heavily encrypted, 2023. URL: https://nixsanctuary.com/dear-telegram-stop-calling-cloud-chats-encrypted-let-alone-heavily-encrypted/.
[8] D. Plakhta, Telegram as a tool for political influence and manipulation, TV and Radio Journalism 19 (2020) 88–94. doi: http://dx.doi.org/10.30970/trj.2020.19.2955.
[9] D. Tarasov, Determining the parameters of botfarm participants' profiles in social networks [Vyznachennya parametriv profiliv uchasnykiv botoferm u sotsial′nykh merezhakh], in: Proceedings of the 11th International Academic Conference ICS-2022, Lviv, 2022, pp. 174-175.
[10] D. Tarasov, O. Peleschyshyn, Experience in solving the problems of overloading the distance learning system during quarantine [Dosvid vyrishennya problem perenavantazhennya systemy dystantsiynoho navchannya pid chas karantynu], in: Proceedings of the 10th International Academic Conference ICS-2021, Lviv, 2021, pp. 118-119. [in Ukrainian]
[11] D. Tarasov, Z. Koval, M. Klymash, Efficiency evaluation of using social networks application in the university e-learning system, CEUR Workshop Proceedings 2392 (2019) 12-22.
[12] F. Chen, Sustainable Education through E-Learning: The Case Study of iLearn2.0, Sustainability 13 (2021).
[13] G. Badea, E. Popescu, A. Sterbini, M. Temperini, Integrating Enhanced Peer Assessment Features in Moodle Learning Management System, in: M. Chang et al. (Eds.), Foundations and Trends in Smart Learning. Lecture Notes in Educational Technology. Springer, Singapore, 2019. https://doi.org/10.1007/978-981-13-6908-7_19.
[14] I. Domazet, V. Simović, The use of Google Analytics for measuring website performance of non-formal education institution, in: Handbook of Research on Social and Organizational Dynamics in the Digital Era, 2020, pp. 483-498.
[15] J. Deep, Telegram Security: Is Telegram safe? Why Crypto companies use Telegram, 2022. URL: https://www.leapxpert.com/telegram-security-is-telegram-safe-why-crypto-companies-use-telegram/.
[16] J. Leyden, Multiple encryption flaws uncovered in Telegram messaging protocol, 2021. URL: https://portswigger.net/daily-swig/multiple-encryption-flaws-uncovered-in-telegram-messaging-protocol.
[17] K. Korsun, Are Telegram and the Kremlin friends or just allies? [Telehram i kreml′ - druzi chy prosto soyuznyky?], 2023. URL: https://enigma.ua/articles/telegram-i-kreml-druzi-chi-prosto-soyuzniki. [in Ukrainian]
[18] M. Mujiono, S. Fatimah, Moodle integration intervention in EFL virtual classroom and academic flow on university students' achievement in writing, Theory and Practice in Language Studies 12(10) (2022) 2182-2190.
[19] M. Tait, Russia is spying on Telegram chats in occupied Ukrainian regions. Here's how, 2023. URL: https://www.pwnallthethings.com/p/russia-is-spying-on-telegram-chats.
[20] P. Fernández-Álvarez, J. Ricardo, J. Rodríguez, Extraction and analysis of retrievable memory artifacts from Windows Telegram Desktop application, Forensic Science International: Digital Investigation 40 (2022).
[21] P. Vostinar, Interactive course for JavaScript in LMS Moodle, Proc. ICETA (2019) 810–815.
[22] Security Analysis of Telegram (Symmetric Part), 2023. URL: https://mtpsym.github.io/.
[23] T. Semerádová, P. Weinlich, Using google analytics to examine the website traffic, in: Website Quality and Shopping Behavior: Quantitative and Qualitative Evidence, Springer, 2020, pp. 91-112.

[24] T. von Arx, G. Kenneth, G. Paterson, On the cryptographic fragility of the Telegram ecosystem, in: Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security, 2023, pp. 328-341.
[25] Tokar.ua, Cooperation with the FSB and servers in Russia - What's wrong with Telegram (ENG sub.), 2023. URL: https://www.youtube.com/watch?v=0V67ADwFsPw.
[26] Y. Vinnichuk, How did a network of anonymous Telegram channels appear in Ukraine [Yak v Ukraini ziavylasia sitka anonimnykh Telegram-kanaliv Dzherelo: https://biz.censor.net/r3151221], 2019, URL: https://biz.censor.net.ua/resonance/3151221/ yak_v_ukran_zyavilasya_stka_anonmnih_ telegramkanalv. [in Ukrainian].