In France, the protection of state secrets at the state level is based on the articles of the Criminal Code, trade secrets are protected by articles of the Criminal Code, Labor and Civil Code. France actively supports countries that have accused Russian intelligence services of cyber attacks on international organizations located on their territory.
The current European organizational structures considered in the study can significantly increase the level of protection against cyber threats not only to the national cyberspace of Germany, but also to most of Germany‟s partner countries due to their clear and efficient interaction.
Key words: information terrorism, Great Britain, Germany, France, information protection, information security, cybersecurity, cyber attack.

REFERENCES

1. Busol O. Osnovni rysy kontroliu za natsionalnym informatsiinym prostorom Korolivstva Velyka Brytaniia. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2962:osnovni-risi-kon trolyu-za-natsionalnim-informatsijnim-prostorom-korolivstva-velika-britaniya-2&catid=71&Ite mid=382.
2. Velikobritaniia raskryla sovershonnye Rossiei kiberataki. URL: https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks.ru.
3. Havrysh, S. B. Kompiuternyi teroryzm: suchasnyi stan, prohnozy rozvytku ta shliakhy protydii. *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka),* 2009, 20.
4. Za rik u Velykii Brytanii zafiksuvaly bilsh nizh 600 kibiratak z boku RF. URL: https://www.5.ua/svit/u-velykii-brytanii-zaiavyly-pro-nevdali-kiberataky-rosiiskoho-hru-pered-otruienniam-skrypaliv-177148.html.
5. Kosilova, O. I. Informatsiina bezpeka Ukrainy v umovakh hlobalizatsii. *Pravova informatyka,* 2010, 3 (27), 27.
6. Yerokhina, T. Media-teroryzm sered inshykh vydiv teroryzmu: sproba typolohichnoho analizu. URL: http://www.social-science.com.ua/article/1002.
7. Minoborony Frantsii podvoit kilkist fakhivtsiv z kiberbezpeky. URL: https://www.dw.com/uk/minoborony-frantsii-podvoit-kilkist-fakhivtsiv-z-kiberbezpeky/a-37057663-0.
8. Sidak V. Orhanizatsiia systemy zakhystu informatsii v Nimechchyni: evoliutsiia ta suchasnyi stan. *Prav., normat. ta metrol. zabezp. systemy zakhystu informatsii v Ukraini,* 2006, 2, 7–11.
9. U Velykobrytanii povidomyly pro suttieve zrostannia kiberahresii z boku Rosii. URL: https://www.unian.ua/ world/1773022-u-velikobritaniji-povidomili-pro-sutteve-zrostannya -kiberagresiji-z-boku-rosiji.html.
10. U Nimechchyni zrostaie kilkist kiberatak na obiekty infrastruktury. URL: https://www.dw.com/uk/u-nimechchyni-zrostaie-kilkist-kiberatak-na-obiekty-infrastruktu ry/a-45841892-0.
11. Chernukhin, I. O. Dosvid Federatyvnoi Respubliky Nimechchyny v pobudovi systemy zakhystu infrastruktury vid kibernetychnykh zahroz. *Informatsiina bezpeka liudyny, suspilstva, derzhavy,* 2014, 1, 27–43.

UDK 351.746:007](8=134)
Piskors'ka Yuliia,
4th year student of Faculty of International Relations
Lesya Ukrainka Eastern European National University,
Lutsk, Ukraine
Yuliia.Piskorska2016@eenu.edu.ua;
Burda Anna,
4th year student of Faculty of International Relations
Lesya Ukrainka Eastern European National University,
Lutsk, Ukraine
Anna.Burda2016@eenu.edu.ua;
Roshko Ivan,
4th year student of
Faculty of International Relations
Lesya Ukrainka Eastern European National University,
Lutsk, Ukraine
Ivan.Roshko2016@eenu.edu.ua

INFORMATION SECURITY IN LATIN AMERICA

Many Latin American companies are not ready to protect their data and are falling behind their international colleagues in terms of cyber insurance adoption. Cybercrime imposes a huge threat for their economies. The states

are experiencing rapid growth, and the rise of digital technology. While this can be considered as a positive change, it opens many possibilities for cyber criminals.
There are only a few countries in this area that have passed cybersecurity-related legislation. There are also the businesses that take care of cyber security, they are slowly entering the market of Latin America countries. Israeli companies are large service providers in the region.
Espionage is one of the strategies that implies intervention in the internal politics of the Latin America states. However, there are other strategies that seem "indirect" and that, nevertheless, can have a great impact in political scenarios, such as cybersecurity in elections.
Three out of five Latin American businesses have suffered a cyberattack. Peru had the highest detection rate, followed by Mexico, Argentina, Brazil, and Colombia, respectively. Al a rule, the leading cause is malicious code. However, in 2018 ransomware took the crown. That rise in ransomware crimes is connected with the fact that it is the cheapest for attackers to facilitate these types of assaults.
To prevent the future massive attacks countries in Latin America & the Caribbean (LAC) started creating their own cybersecurity strategies. Chile and Mexico published their Cybersecurity Strategies in 2017, and have taken into account a broad spectrum of cybercrime aspects to address cybersecurity risks in order to create a comprehensive framework.
In case with cybersecurity, as in every field, cooperation plays a fundamental role. Latin American countries have been partnering up to build better ties in respect to cybersecurity. One of the platforms that was used for building such partnerships was the XIII Pacific Alliance Summit that took place in Mexico.
The Organization of American States (OAS) has been centrally engaged with issues of cybersecurity and cybercrime for over a decade, encouraging and supporting the work of Member States to strengthen their capacity to protect the people, economies, and critical infrastructure of our region against cybercrime and other cyberattacks or incidents.
Key words: *information space, information security, cyberattack, cybersecurity, cybercrime, Latin America, Brazil, Mexico, Chile.*

1. INTRODUCTION

As the Internet experienced its rapid expansion in the 1990s, hackers began engaging in cyber «pranks» while low-level criminals began exploring the potential for cybercrime. Once it was shown that «crime pays» in the cyber domain, organized crime began muscling its way onto the scene, in some cases apparently with the blessing – and even support – of the governments on whose territory they were operating.

Before exploring the topic of Information security in Latin America, it is important to consider some basic vocabulary terms: *Information Space* – is a collection of information that is not limited by source, form, process, semantics, or application. *Information Security* is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electrical one. A *cyber attack* – an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. As described by Cisco, «a cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization» [1].

The most common types of cyberattacks are phishing, data breach, malicious code, software exploit, in addition to ransomware. *Phishing* – the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. *Data breach* – the intentional or unintentional release of secure or private / confidential information to an untrusted environment. *Malicious code* – software intentionally designed to cause damage to a computer, server, client, or computer network. *Ransomware* – a type of malicious software designed to block access to a computer system until a sum of money is paid. *Propaganda* – information, ideas, opinions, or images, often only giving one part of an argument, that are broadcast, published, or in some other way spread with the intention of influencing people‟s opinions [2, 3, 4].

Problem statement. In the world rank of countries affected by cyber attacks there are several Latin American nations. Brazil occupies the seventh place and Mexico the eleventh. According to the Kaspersky (antivirus company), Colombians receives an average of 3.8 cyber attacks per second. Argentina and Chile – 0.8, and Peru – 2.14. This data is an approximation based on people connected to the internet in each country and using Kaspersky [6].

Cybercrime imposes a huge thread for Latin American economies. The states are experiencing rapid growth, and the rise of digital technology. While this can be considered as a positive change, it opens many

possibilities for cyber criminals. For example, in Colombia, only 3 percent of the population used the Internet in 2000, but now more than half of population went online. Many Latin American companies are not ready to protect their data and are falling behind their international colleagues in terms of cyber insurance adoption. There are only a few countries in this area that have passed cybersecurity-related legislation [5].

2. RESEARCH RESULTS

Mexico has implemented the law to provide more strict penalties for data breaches, Brazil has lost approximately $8 billion as the result of cybercrime but has not yet passed a general data protection law. Brazil is currently a popular target for increased use of malware designed to infect systems. According to an Eset Latin American Security Report (2017) cyber attacks in Brazil increased 197% in 2015, and a survey of Brazilian companies revealed that one-third had experienced a cybercrime. On the behalf of the governments, businesses in Latin America are not required to improve their cybersecurity measures. This can easily cause company leaders to underestimate the threats they now face, as well as the potential consequences of a serious data breach. Not only it effects big corporations but also small business and individuals, many are simply uninformed about the virtual about the threats [7].

The consulting firm "Return Comstor" expects that in 2019 the Latin American cybersecurity market will reach 12 trillion dollars. Fortinet is one of the leading companies in providing internet protection services. Only in Peru it covers just over 60% of devices protected by its services. Peru is followed by Brazil, Colombia, Chile, Mexico, Venezuela and Argentina [8].

Slowly, there are the businesses that take care of cyber security, they are entering the market of Latin America countries. Israeli companies are also large service providers in the region. Verint and Elbit are the most prominent cybersecurity service providers and, in the particular case of Mexico, the introduction of software of this type has been used by the Enrique Peña Nieto government to spy on journalists and opponents. One of the privileged clients of Israeli cybersecurity is Brazil, a market that it shares with the United States, and which is in the process of expansion with the Government of Jair Bolsonaro. Indeed, one of the objectives set by the Innovation Group, sponsored by IBM, of the Brazil US Business Council (main business lobby organization dedicated to strengthening the economic and commercial relationship between Brazil and the US), is to support the adoption of regulations in Brazil that promote a flexible and innovation-based approach to cyber security and public-private discussions on cyber best practices and the threat of information exchange [9].

Not least is that, despite the espionage scandal by the US National Security Agency to the Dilma Rousseff government, cooperation with the US has deepened. Specifically in areas such as e-government, cyber security, and cyber crime prevention. In 2016, while the impeachment process was progressing, the Brazilian Ministry of Science, Technology and Innovation and the US National Science Foundation, USA signed a memorandum of cooperation on cybersecurity. After the coup was completed, Michel Temer announced the hiring of software created by Microsoft and, within this framework, the company opened a Transparency Center in Brazil that allows governments have access to information related to cyber security.

Espionage is one of the strategies that implies intervention in the internal politics of the Latin America states. However, there are other strategies that seem "indirect" and that, nevertheless, can have a great impact in political scenarios, such as cybersecurity in elections. The Brazilian elections that brought Bolsonaro to the Presidency seem to be an example of this [10].

According to the survey conducted by the Internet resource Contxto among Mexico, Colombia and Brazil, significant cyber-attacks came via email, transpired through malicious websites, via software, and from external devices (fig. 1).

A security report on Latin America provided by ESET (cyber protection) talks about how cyberattacks have increased in the region. Three out of five Latin American businesses have suffered a cyberattack. Peru had the highest detection rate, followed by Mexico, Argentina, Brazil, and Colombia, respectively. Al a rule, the leading cause is malicious code. However, in 2018 ransomware took the crown. That rise in ransomware crimes is connected with the fact that it is the cheapest for attackers to facilitate these types of assaults. Overall, 57 percent of companies received ransomware attacks. 55 percent of businesses underwent data breach and malware affected 53 percent of organizations [11].

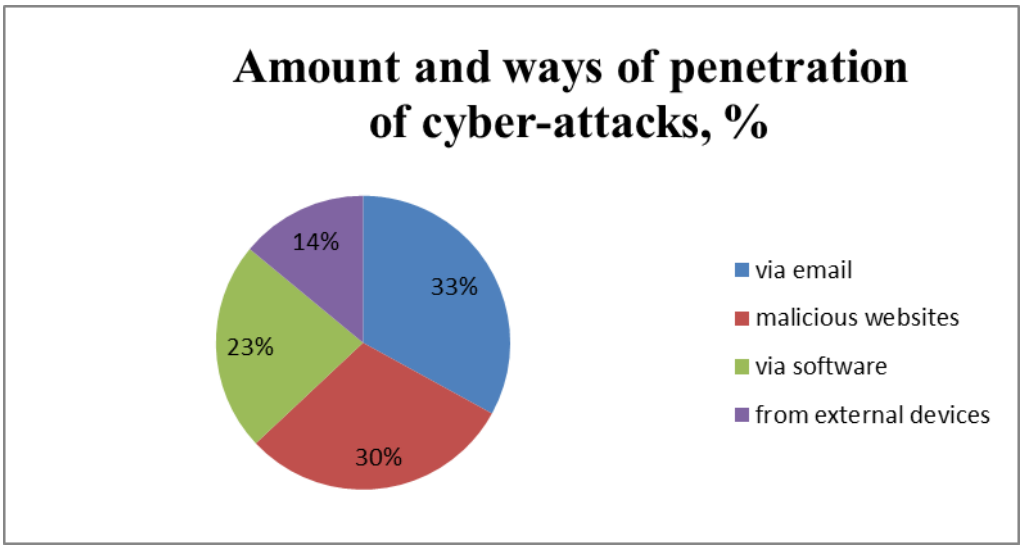

Fig. 1. *Ways of penetration of cyber-attacks (according to the survey conducted by the Internet resource Contxto among Mexico, Colombia and Brazil) [2]*

A good example of huge damage done by cyberattacks is the case in Banxico, Mexico‟s central bank, in which 836 bank accounts from 10 different institutions were victims of fraud, and the attack had a cost of roughly almost 16 million USD. Another example, in Brazil, Banco Inter was hacked and sensitive information was leaked, falling 11% in market shares. In Chile, Banco de Chile was also target of a cyberattack, where the hackers stole 10 million USD [12].

To prevent the future massive attacks countries in Latin America & the Caribbean (LAC) started creating their own cybersecurity strategies. Chile and Mexico published their Cybersecurity Strategies in 2017, and have taken into account a broad spectrum of cybercrime aspects to address cybersecurity risks in order to create a comprehensive framework. Mexico will specifically focus on economy and innovation, civil society and rights, public security, national security, and public institutions, while Chile seeks to improve their infrastructure, people‟s rights in cyberspace, develop a cybersecurity culture, cooperation, and promotion of the cybersecurity industry [13].

Argentina took a similar approach and created a program called "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad". With this program, Argentina seeks to improve the creation and adoption of a regulatory framework for the identification and protection of key infrastructures, be it private or governmental, against cyber-threats.

The Organization of American States (OAS) has been centrally engaged with issues of cybersecurity and cybercrime for over a decade, encouraging and supporting the work of Member States to strengthen their capacity to protect the people, economies, and critical infrastructure of our region against cybercrime and other cyberattacks or incidents. In 2004 the OAS Member States adopted the Inter-American Integral Strategy to Combat Threats to Cyber Security, which called for a coordinated, multi-stakeholder effort to countering cyber threats in the hemisphere, and provided an initial framework to cultivate and guide such an approach. The Member States showed great foresight in embracing this vision early. The Organization creates a space where meaningful cooperation between a wide range of stakeholders has improved information sharing, enhanced the protection of information and communications technology (ICT) infrastructure, strengthened our governments‟ capacity to respond to and mitigate cyber incidents, and bolstered our individual and collective resiliency in the face of cyber threats. These commitments have been reaffirmed and strengthened in the years since with the adoption of numerous official declarations.

In case with cybersecurity, as in every field, cooperation plays a fundamental role. Latin American countries have been partnering up to build better ties in respect to cybersecurity. One of the platforms that was used for building such partnerships was the XIII Pacific Alliance Summit that took place in Mexico between the 23rd and 28th of July. During the Summit, the presidents of Brazil, Chile, and Mexico talked about strengthening collaboration in cybersecurity, among other matters. The Summit, being of an economical nature, is concerned about the cyberspace, and thus making it a new high priority issue [14].

3. CONCLUSIONS AND PROSPECTS OF FURTHER RESEARCH

Awareness of the importance of developing cybersecurity strategies is increasing among countries in the Latin American and Caribbean (LAC) region. Some of them already have a strategy in place, such as Colombia, Jamaica, Panama, and Trinidad and Tobago. Other countries are in the process of developing one, such as Costa Rica, Dominica, Peru, Paraguay and Suriname. The level of maturity of these strategies varies, including in terms of providing a framework for cooperation among governmental agencies and with external actors. In the LAC region, the army and the national security agencies have not been widely established as coordinators of cybersecurity policy development. This provides a positive window of opportunity to develop cybersecurity policies in multi-stakeholder platforms, including different governmental branches, academia, the technical community, civil society, and the private sector.

In the leadoff the chart of the countries that have suffered the biggest number of cyber attacks are Brazil and Mexico; however, they are also the ones that have the most regulation. In case with Brazil, the private sectors have experienced particular damage. Therefore, the government had established well-functioning National Data Protection Authority. Mexico has suffered major losses in public sector, as there were cyber attacks on the financial institutions. Still, the country has not developed the sufficient cyber crime prevention mechanism. Argentina is the next in line to have experienced cyber crime. Recently the official pages of governmental were hacked and used to spread fake news along with links of stolen information; however, the government did not address the issue publically. There is a sense of presence of Russian propaganda in the region well as USA influences in the Media. In particular around Columbian and Venezuelan conflict, both superpowers were noticed to be engaged in the social media activities around the time of Venezuelan election. Nonetheless, most of the countries of the region unite their forces in a battle again cyberattacks, participating in the International events dedicated to the issue.

REFERENCES

1. What Are the Most Common Cyber Attacks? URL: https://www.cisco.com/c/en/us/ products/security/common-cyberattacks.html.
2. Cyber attacks in Latin America – the growing need for digital security. URL: https://www.contxto.com/ en/informative/cyber-attacks-in-latin-america-the-growing-need-for-digital-security/.
3. IGI Global. What is Information Space. URL: https://www.igi-global. com/dictionary/visual-analytics-conceptual-blending-theory/14513.
4. GeeksforGeeks. Information System and Security. URL: https://www.geeksfor geeks.org/what-is-information-security/.
5. The role of cybersecurity in world politics. URL: https://www.researchgate.net/ publication/316949336_ The_role_of_cybersecurity_in_world_politics.
6. Risk of data breaches, cybercrime growing in Latin America. URL: https://terranovasecurity.com/risk-of-data-breaches-cybercrime-growing-in-latin-america/
7. Latest news about information vulnerabilities, threats, incidents and events. URL: https://h-xtech.com/news-industry.
8. Así está la ciberseguridad en América Latina. URL: https://www.elespectador.com/ tecnologia/asi-esta-la-ciberseguridad-en-america-latina-articulo-878632.
9. Ciberseguridad, un desafío para América Latina y el Caribe. URL: https://www.celag.org/ciberseguridad-un-desafio-para-america-latina-y-el-caribe/.
10. Types of Cyber Attacks. URL: https://co.pinterest.com/pin/85455809803020 9762/?amp_client_id= CLIENT_ID(_)&mweb_unauth_id=%7B%7Bdefault.session%7D%7D&simplified=true.
11. Most common types of offline cyber attack types in Latin America in 2017. URL: https://www.statista.com/ statistics/818458/most-common-types-offline-cyber-attacks-latin-america/.
12. CYBERSECURITY CHALLENGES FOR LATIN AMERICA. URL: https://www.seguridadinternacional.es/ ?q=es/content/cybersecurity-challenges-latin-america.
13. Cybersecurity. Are We Ready in Latin America and the Caribbean? URL: https://publications.iadb.org/ publications/english/document/Cybersecurity-Are-We-Ready-in-Latin-America-and-the-Caribbean.pdf.
14. The Next Generation of Cybersecurity in Latin America. URL: https://www.fairobserver.com/region/ latin_america/cybercrime-cybersecurity-latin-america-news-world-news-now-76839/.

Матеріал надійшов до редакції 03.12.2019 р.

ІНФОРМАЦІЙНА БЕЗПЕКА В ЛАТИНСЬКІЙ АМЕРИЦІ

Багато латиноамериканських компаній не готові захищати дані й відстають від своїх міжнародних колег щодо прийняття кіберстрахування. Кіберзлочинність становить величезну загрозу для їхньої економіки. Держави відчувають стрімке зростання цифрових технологій. Хоча це може розглядатися як позитивна зміна – воно відкриває багато можливостей і для кіберзлочинців.

У цій галузі є лише кілька країн, які прийняли законодавство про кібербезпеку. Існують також підприємства, які піклуються про кібербезпеку, вони повільно виходять на ринок країн Латинської Америки. Ізраїльські компанії є великими постачальниками послуг урегіоні.

Шпигунство – одна зі стратегій, що передбачає втручання у внутрішню політику держав Латинської Америки. Однак є й інші стратегії, які видаються «непрямими», а, утім, можуть надто впливати на політичні сценарії, як-от кібербезпека на виборах.

Три з п‟яти латиноамериканських підприємств зазнали кібератак. Найвищий показник виявився в Перу, за ним – Мексика, Аргентина, Бразилія та Колумбія. Зазвичай, головною причиною є шкідливий код. Однак у 2018 р. вірус-вимагач забрав корону собі. Зростання кількості злочинів, що вимагають викупу, пов‟язане з тим, що для зловмисників це найдешевший спосіб просування й сприяння нападам.

Для запобігання майбутнім масовим атакам країни Латинської Америки та Карибського басейну почали створювати власні стратегії кібербезпеки. Чилі й Мексика опублікували свої стратегії кібербезпеки у 2017 р. та врахували широкий спектр аспектів кіберзлочинності для подолання ризиків кібербезпеки задля створення всеосяжної системи.

У разі кібербезпеки, як і в усіх галузях, співпраця відіграє принципову роль. Латиноамериканські країни співпрацюють для створення кращих зв‟язків щодо кібербезпеки. Однією з платформ, які використовувались для побудови таких партнерств, був XIII саміт Тихоокеанського альянсу, що відбувся в Мексиці.

Організація американських держав уже понад 10 років займається однією з основних проблем кібербезпеки та кіберзлочинності, заохочуючи й підтримуючи роботу держав-членів щодо посилення їх спроможності стосовно захисту людей, економіки та критичної інфраструктури регіону від кіберзлочинності й інших кібератак чи інцидентів.

Ключові слова: інформаційний простір, інформаційна безпека, кібератака, кібербезпека, кіберзлочинність, Латинська Америка, Бразилія, Мексика, Чилі.

УДК 316.485.26:316.776.23(470)

Тихомирова Євгенія,
доктор політичних наук, професор,
Східноєвропейський національний університет імені Лесі Українки,
Луцьк, Україна, teb53@ukr.net
https://orcid.org/0000-0002-5017-5875

РОСІЙСЬКА ІНФОРМАЦІЙНА ВІЙНА: ТЕОРЕТИЧНІ ТА ПРАКТИЧНО-ПРИКЛАДНІ АСПЕКТИ

У статті розглянуто проблему наростання інформаційної війни, що виникла внаслідок агресивної політики Росії та створила небезпеку як сучасному європейському, так і українському інформаційному простору. Посилаючись на аналіз результатів наукових досліджень, за допомогою яких вивчались окремі теоретичні та практично прикладні аспекти цієї війни, говоримо про сутність досліджуваної проблеми й потребу її розв'язання.

Мета даної публікації – 1) проаналізувати термін «російська інформаційна війна» (трактується як комплекс заходів, здійснюваних урядовими та неурядовими організаціями Росії, передусім в інформаційному просторі України й Росії, інших країн світу); 2) виокремити місце інформаційної війни в російській геополітичній доктрині, котра розглядається як система офіційно прийнятих у державі поглядів на розвиток світових процесів, міжнародну систему безпеки, утвердження геополітичних інтересів і пріоритетів РФ у сучасному світі, їх реалізація та захист; 3) охарактеризувати особливості російських військ для «інформаційних операцій», спеціальних підрозділів для ведення інформаційної боротьби в