INFORMATION SECURITY AT ASEAN IN A DIGITALIZED ECONOMY: NATIONAL AND REGIONAL APPROACHES

DOI: https://doi.org/10.24115/S2446-622020206Extra-A656p.214-221

Ella V. Gorian[i]

ABSTRACT

The article describes features of the regulatory and institutional mechanisms of cybersecurity at the national and regional levels and determines the role of the leading states of the region in shaping the digitalization vector of the economy. The methodological basis of the study includes systemic-structural, formal-logical and hermeneutical methods of scientific knowledge using special legal methods of cognition (comparative legal and historical legal). The national approaches of ASEAN member states in information security are determined by many factors, which affects the level of security in a specific state. The unification of standards will help achieve several goals: the sustainability of the digital economic system of the region, the growth of the qualitative and quantitative level of training, the increase in the investment attractiveness of the financial sector, and simplification of the procedures for creating FinTech companies.

Keywords: Digital economy. Cybersecurity. ASEAN. Investment banking. Critical information infrastructure.

SEGURANÇA DA INFORMAÇÃO NA ASEAN EM UMA ECONOMIA DIGITALIZADA: ABORDAGENS NACIONAIS E REGIONAIS

LA SEGURIDAD DE LA INFORMACIÓN EN LA ASEAN EN UNA ECONOMÍA DIGITALIZADA: ENFOQUES NACIONALES Y REGIONALES

RESUMO

O artigo descreve características dos mecanismos regulatórios e institucionais de cibersegurança em nível nacional e regional e determina o papel dos principais estados da região na formação do vetor de digitalização da economia. A base metodológica do estudo inclui métodos sistêmico-estruturais, lógico-formais e hermenêuticos do conhecimento científico usando métodos jurídicos especiais de cognição (jurídico comparativo e jurídico histórico). As abordagens nacionais dos estados membros da ASEAN em segurança da informação são determinadas por muitos fatores, que afetam o nível de segurança em um estado específico. A nível regional, as iniciativas até agora cobrem o aspecto da política externa e consistem no estabelecimento de relações sustentáveis, cooperação interinstitucional e assistência mútua. A unificação de padrões ajudará a atingir diversos objetivos: a sustentabilidade do sistema econômico digital da região, o crescimento do nível qualitativo e quantitativo de formação, o aumento da atratividade de investimentos do setor financeiro e a simplificação dos procedimentos de criação Empresas FinTech.

Palavras-chave: Economia digital. Cibersegurança, ASEAN. Banco de investimento. Infraestrutura de informação crítica.

RESUMEN

El artículo describe características de los mecanismos regulatorios e institucionales de la ciberseguridad a nivel nacional y regional, y determina el papel de los estados líderes de la región en la conformación del vector de digitalización de la economía. La base metodológica del estudio incluye métodos de conocimiento científico sistémico-estructural, formal-lógico y hermenéutico utilizando métodos legales especiales de cognición (legal comparado e histórico legal). Los enfoques nacionales de los estados miembros de la ASEAN en seguridad de la información están determinados por muchos factores, lo que afecta el nivel de seguridad en un estado específico. A nivel regional, las iniciativas hasta ahora abarcan el aspecto de la política exterior y consisten en establecer relaciones sostenibles, cooperación interinstitucional y asistencia mutua. La unificación de estándares contribuirá al logro de varias metas: la sustentabilidad del sistema económico digital de la región, el crecimiento del nivel cualitativo y cuantitativo de capacitación, el aumento del atractivo inversor del sector financiero y la simplificación de los procedimientos de creación.

Palabras-clave: Economía digital. Ciberseguridad. ASEAN. Banca de inversión. Infraestructura de información crítica.

INTRODUCTION

The reported study was funded by RFBR, project number 20-011-00454 "Ensuring the rights of investors in the banking and financial sectors in the context of the digitalization of the economy in the Russian Federation and the leading financial centers of East Asia: a comparative legal aspect".

RELEVANCE

In recent years, the countries of Southeast Asia have shown a sharp increase in the digital economy. In their report "e-Conomy SEA Spotlight 2017: Unprecedented growth for Southeast Asia's $ 50B internet economy", Google and Temasek analysts estimated the regional digital economy market in 2017 at $50 billion, which exceeded all experts' expectations (e-Conomy SEA Spotlight: Unprecedented growth for Southeast Asia's $50B internet economy (report by Google and TEMASEK. 2017). In particular, by the end of 2017, the number of Internet users amounted to more than 330 million people, showing an increase of 70% compared to 2015. More than 90% of these users use smartphones to access the Internet and spend about 3.6 hours a day on mobile Internet, which is much more compared to users from other regions.

Such a sharp growth in the digital economy of Southeast Asia is associated with the successes of six companies, each estimated at approximately $1 billion: 1) Grab Holdings: a developer of mobile transport applications such as Grab Taxi, GrabCar, GrabBike, GrabExpress, used in all countries of Southeast - East Asia; 2) Traveloka: a leader in hotel and airline reservations; 3) Tokopedia: Indonesia's leading e-commerce platform; 4) Go-Jek: a multidisciplinary mobile application (transport, food delivery, transportation, payments, various services); 5) SEA Group: a platform for electronic commerce, digital entertainment, electronic payments; 6) Lazada: a leading e-commerce platform in Southeast Asia. The growth of the digital economy is mainly associated with the development of four main industries: 1) hotel and airline booking (26.6 billion US dollars in 2017, which shows an increase of 18% compared to 2015); 2) online media (6.9 billion US dollars in 2017, an increase compared to 2015 amounted to 36%); 3) electronic commerce (11 billion US dollars with an increase in the volume of operations by 41% compared with 2015); and 4) transport services (5 billion US dollars and an increase of 100% compared to 2015) (e-Conomy SEA Spotlight: Unprecedented growth for Southeast Asia's $50B internet economy [report by Google and TEMASEK]. 2017).

Such impressive growth rates make it necessary to harmonize the laws of the member states of the Association of Southeast Asian Nations (hereinafter - ASEAN). Five ASEAN members (Vietnam, Indonesia, Malaysia, Singapore, and Thailand) have already joined the so-called ASEAN Single Window, an online platform for expedited customs clearance through electronic exchange of trade documents for cross-border transactions. The next step is the harmonization of electronic commerce rules, consumer protection standards, personal data protection, antitrust policy and cybersecurity, and the development of a legal framework for the Internet dispute settlement (IWAMOTO, 2018).

Among ASEAN member states, Singapore plays a key role in the integration process. As the most developed state in information technology in the world, Singapore is also a key international financial and trade center. This makes it an ideal target for cyberattacks, the consequences of which are much more serious than the usual violation of Singapore's public and economic well-being - the entire international supply chain and the banking sector, and, in the long term, the international economy, will go under blow. Therefore, in 2016, Singapore developed one of the best national cybersecurity strategies to date (National Cybersecurity Strategy 2016, hereinafter - NCS), and in 2018, the Singapore Parliament adopted the Cybersecurity Act 2018 (hereinafter - CSA), which is considered a new generation standard for the protection of key information infrastructure (hereinafter - CII), which makes it the object of close attention of professionals from various fields.

In 2018, at the 32nd annual ASEAN Member States Summit in Singapore, the member states emphasized such a key aspect of cooperation as cybersecurity, due to the increased nature and scale of cyber-attacks. In their statement, the ASEAN Heads of State addressed relevant ministers about the need to consider all possible ways to coordinate cyber security, diplomacy and technical cooperation at different levels of the three pillars of ASEAN: ASEAN Political Security Community (APSC), ASEAN Economic Community (AEC), and ASEAN Socio-Cultural Community (ASCC). Heads of the ASEAN state recognize the effectiveness of the ASEAN Cyber Capacity Program, initiated in 2016 by Singapore (par. 6) (Chairman's Statement of the 32nd ASEAN Summit Singapore, 28 April 2018). The growth of FinTech companies in the region requires a review of existing approaches to ensuring information security at the national and regional levels. All of the above indicates the relevance of the research topic.

PROBLEM STATEMENT

Digitalization of the economy puts the state and society in need of ensuring the security of information technologies that serve companies and consumers. Each state is developing its own approach, subject to the many inherent factors. But the interconnection of national economies within the framework of the integration association, which is ASEAN, forces us to develop a unified regional approach that will solve not only the problem of information security, but also others - qualitative and quantitative training of personnel, simplification of modes for the functioning of FinTech companies.

METHODS

The methodological basis of the study includes systemic-structural, formal-logical and hermeneutical methods of scientific knowledge using special legal methods of cognition (comparative legal and historical legal).

LITERATURE REVIEW

A number of scientific studies by scientists from Singapore and China consider the organizational, legal and technical features of ensuring the information security of financial and banking systems in the aspect of a decentralized approach (each subject is separate from the whole system) (BALUTA, RAMAPANTULU, CHANG, 2017; TER, 2018), however, in a case of outsourcing of processes, as it actually takes place, the vulnerability of the banking system becomes a decisive factor determining the need for centralized development of outsourcing standards, including in the case of using the so-called cloud technologies.

Some Singapore researchers pay attention to this, but from the technical side of the problem (CHALLA, 2018; LI, et al. 2019), leaving out of sight its organizational and legal aspects. An important point in ensuring cybersecurity is a risk management system that allows you to allocate all available resources depending on a particular scenario of negative impact on the operating systems of financial and banking institutions (ZHANG, HE, CHOW, 2018). As for the regional approach to ensuring cybersecurity under the digitalization of the economy, the studies conducted by industry experts who publish regular reviews of regional and national approaches in terms of their effectiveness in countering quantitative and qualitative cyber threats are of interest [RAJ, 2020).

RESULTS

International law provides no unambiguous definition of a critical information infrastructure (CII) in international law, so each state sets criteria for defining any data, databases, networks, telecommunications infrastructure (or part thereof) as CII. Some states have already identified their CII sectors and have embarked on a phase of ensuring their security, while others are just embarking on a definition phase (MATTIOLI, 2014). This leads to a difference in national CII protection mechanisms depending on information assets, powers of authorities, regulatory methods, etc.

For example, Thailand, in Section 49 of the Cybersecurity Act, identifies the following sectors of CII: (1) national security; (2) substantive public service; (3) banking and finance; (4) information technology and telecommunications; (5) transportation and logistics; (6) energy and public utilities; (7) public health; (8) others as prescribed by the Committee (Cybersecurity Act 2019). Malaysia's CII objects are grouped into 10 sectors: (1) national defense & security; (2) banking & finance; (3) information & communications; (4) energy; (5) transportation; (6) water; (7) health services; (8) government; (9) emergency services; (10) food & agriculture (https://cnii.cybersecurity.my/main/about.html).

As a rule, states identify the CII sectors and their key protection factors in respective strategies and enshrine the cybersecurity mechanism in a special law. ASEAN member states has the following the regulatory situation. In Vietnam, until June 2018, there was no regulatory act on cybersecurity. On January 1, 2019, the Law on Cybersecurity adopted in June 2018, which international human rights organizations and business associations have already called a threat to civil and economic freedoms, will come into force (NGUYEN, 2018). In Indonesia, cybersecurity legislation is being drafted (a draft Law on Information Technology and Electronic Transaction, ITET is being drafted). Currently, the Law of 2008 in the 2016 edition of the Law on Information and Electronic Transaction, which has many gaps and cannot cope with modern cyber threats, is in force (Cybersecurity: Indonesia. 2018).

Malaysia has the second oldest Computer Crime Act 1997 among ASEAN member states. Other special laws include the Personal Data Protection Act 2010; in 2016, the National Cybersecurity Policy 2016 came into force, which defined the CII sectors, a year later the development process began cybersecurity law. Thailand is one of the twenty countries in the world with a leading position in ensuring cybersecurity (Cybersecurity: Indonesia. 2018). For more than a decade now, the Computer Crimes Act 2007 (revised in 2017) and the Personal Data Protection Act 2018 have been in force in the country, and a hearing is underway on the approval of the National Cybersecurity Bill and the national cybersecurity strategy.

In 2017, the Philippines began to implement the National Cybersecurity Plan 2022, which identified CII sectors. Since 2012, the Cybercrime Prevention Act 2012 and the Data Privacy Act 2012 have been in force. Other ASEAN states (Brunei Darussalam, Cambodia, Laos, Myanmar) have no developed national cybersecurity strategies and relevant legislation (with the exception of Laos, which has begun to develop a package of laws on cybercrime).

Singapore was the first state in ASEAN to adopt the Computer Misuse and Cybersecurity Act 1993 (revised in 2017) in 1993. Today, the cyber security legislation of this country is presented in the Personal Data Protection Act 2012, the National Cybercrime Action Plan 2016, the National Cybersecurity Strategy 2016, and Cybersecurity Act 2018. Experts note the "soft focus" policy of integration processes in cybersecurity in ASEAN by Singapore (https://www.cisco.com/c/dam/m/en_sg/cybersecurity/cybersecurity): for example, the government initiated the headquarters in Singapore of the INTERPOL Global Complex for Innovation (IGCI), a research center that focuses on cybercrime, innovative training, operational support and partnerships, and also proposed as part of ASEAN's collaboration with Interpol to allocate more law enforcement officers to ASEAN member states to serve at IGCI.

In addition, Singapore, together with Japan and the United Kingdom, was the founder and sponsor of the non-profit cooperation organization - The CyberGreen Institute (https://www.cybergreen.net). This institution collects and provides reliable statistics, measurements and best practices for mitigating the effects of cyber-attacks on interested telecom operators, national Cyber Security Incident Response Teams (CSIRTs), and national and international cyber security policy makers. As part of the CyberGreen project, ASEAN states receive information on the status and potential vulnerabilities of cyber defense, which allows them to prevent potential cyber risks. Over time, it is planned to develop a reliable cyber defense methodology. This will draw the balance of how each state and ASEAN as a whole respond to cyber threats, which will be systematized by hazard class, so it will be easier for national cyber response teams to develop a strategy and tactics of counteraction, considering the information provided by CyberGreen specialists.

As a sponsor of this initiative, Singapore provides ASEAN member states with free access to CyberGreen project data, as well as the first report on the status of the national cybersecurity system. This will allow the states of the region to improve their joint efforts to create secure ASEAN cyberspace. Recently, Malaysia has competed with Singapore for leadership in the region in conducting national initiatives to strengthen cybersecurity. A recent study showed that Malaysian companies were much more likely than companies in any other APAC region to identify safety regulations as affecting their organizations. Malaysia also led all countries in identifying privacy regulations as impacting organizations (85% of respondents). This comes in stark contrast with Singapore, which is the country with the highest estimated costs stemming from cybersecurity incidents in the APAC region over the last twelve months.

The financial regulators of some ASEAN countries have implemented internationally recognized models of cybersecurity systems, including those developed by the National Institute of Standards and Technology (NIST), the Bank of England (CBEST) and the United States Federal Financial Exam Council. Many also use common international standards for assessing safety and compliance, including ISACA COBIT and the ISO/IEC 27000 series (CARTER, CRUMPLER, 2019, p. iv).

The implementation of these standards was carried out given their own national factors, which led to the appearance of similar, but not necessarily complementary regulatory and supervisory regimes for multinational financial institutions. However, according to researchers, the establishment of common agreed regional standards will allow for better management of systemic risk, increase in regulatory efficiency and a basic level of security and protection within the regional financial system, especially in small countries with limited cyber security capabilities (CARTER, CRUMPLER, 2019, p. 42).

In addition, harmonization of national cybersecurity standards will solve the problem of labor. Eliminating redundant requirements for security assessment, audits, and penetration tests can make more cybersecurity professionals available for other tasks, such as operational security in financial institutions and oversight and

examination functions in regulatory bodies. The establishment of common standards, certification requirements and reporting regimes can simplify the regional system of training, obtaining the necessary skills, experience and certification, as well as allow existing employees to support security operations and compliance with regulatory requirements in various jurisdictions (CARTER, CRUMPLER, 2019, p. 42). Such harmonization of standards is a matter of time and the willingness of ASEAN member states to dialogue and unification of national approaches into a single common, regional one.

Currently, the current regional approaches are aimed primarily at coordinating the foreign policy. Thus, the ASEAN Regional Forum (ARF) is the ASEAN Special Security Tool. This institutional mechanism refers to the tools of "preventive diplomacy" and operates at two levels - intergovernmental and non-governmental (non-governmental organizations and academia participate). The result of the ASEAN Regional Forum on Security is a series of program documents (work plans), including the safety and use of information and telecommunication technologies (ARF Work Plan on Security of and in the Use of Information and Communications Technologies). This document was adopted in 2015 (http://aseanregionalforum.asean.org/wp-content/uploads/2018) and provides for two types of activities that are carried out by collaborating parties: 1) creation and participation in an open-ended research group on confidence-building measures to reduce the risk of conflicts related to the use of ICTs.

Such a research group should (a) develop information sharing processes and procedures between participants on the prevention of ICT crises and the use of ICT for criminal and terrorist purposes, and (b) create and constantly update databases (without duplicating the activities of computer response teams for emergencies - CERT); 2) holding of workshops and seminars for participants, the focus of which should be on the following aspects:

(i) voluntary exchange of information on national legislation, best practices and strategies, as well as rules and regulations regarding the safety and use of ICT, as well as procedures for such exchange of information;

(ii) a discussion on the prevention of security incidents and the use of ICTs;

(iii) conducting of research on the use of ICTs and the prevention of security threats while creating databases of potential threats and possible remedies, considering the work already done in the commercial computer security sector and computer emergency response teams - CERT;

(iv) building of capacity related to the security and use of ICTs, as well as countering of the criminal use of the Internet; (v) promotion and collaboration in research and analysis on issues related to the safety and use of ICTs;

(vi) discussion of the rules, norms, and principles of responsible behavior of participating countries and the role of cultural diversity in the use of ICTs;

(vii) raising of awareness of non-technical personnel and politicians about the threats posed by the use of ICTs and how to counter such threats;

(viii) measures to promote cooperation between the participating countries in combating the criminal and terrorist use of ICTs, including, in particular, cooperation between law enforcement agencies and practicing lawyers, the possible creation of joint groups to prevent crime and exchange information on a possible mechanism for regional cooperation;

(ix) a discussion of terminology related to the security and use of ICTs to facilitate understanding of various national practices;

(x) consideration of the establishment of a contact center for member countries to facilitate real-time communication of events and incidents related to the security and use of ICTs that are potentially important for regional security;

(xi) consideration of the establishment of channels for online exchange of information on ICT threats, global ICT incidents and sources of ICT attacks that threaten critical information infrastructure, and the development of real-time information exchange methods (using emergency computer response teams) situations - CERT). As part of the implementation of this plan, Malaysia is actively involved in organizing events and developing key strategies.

As the above review shows, security is one of the important aspects of ASEAN cooperation. The main emphasis was initially placed on countering terrorism and its financing, including in the area of information and computer technologies. However, in recent years, there has been growing concern about information security not only in terms of the fight against terrorism, but also in terms of ensuring the stability of the digital economy, as well as establishing political and power advantage in regional disputes relating, first of all, to maritime territories in the South China Sea. We shall consider the latest ASEAN regional cybersecurity approaches.

In 2018, the ASEAN Ministerial Conference on Cybersecurity (AMCC) and the ASEAN Telecommunications and Information Technology Ministers' Meeting, TELMIN, as well as the relevant breakout sessions of the ASEAN Ministerial Meeting on Transnational Crime, AMMTC the following arrangements were made. First, participants of the ASEAN Ministerial Conference on Cybersecurity agreed to support and implement 11 voluntary and non-binding norms, rules, and principles of responsible behavior by states to help ensure an open, safe, stable, accessible and peaceful information environment, as proposed in the Report of the Group of Governmental Experts on Achievements in the field of informatization and telecommunications in the context of international security of the United Nations ICT environment in 2015 (Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015). Specialists explain this unanimous readiness of ASEAN states to implement the 11 standards as a result of Singapore's foreign policy initiatives within ASEAN. Until recently, a discussion of regional international norms seemed unthinkable in Southeast Asia, since the region's priorities were focused on combating cybercrime, as well as on monitoring and combating criminal content (for example, as mentioned above, with the promotion of the ideology of terrorism).

Cyberspace in terms of international security was considered exclusively in the aspect of the use of the Internet by terrorists (NOOR, 2018). However, the declaration of readiness to comply with these 11 international standards may remain unimplemented, “on paper”, because, despite the assurances of all actors about cooperation and mutual support, states are objectively not ready to communicate with “open visors”: the level of tension in the region is growing due to unresolved territorial disputes in the South China Sea, work “against all” intelligence services, collection of “sensitive” information about political forces and business circles, etc. (Southeast Asia: An Evolving Cyber Threat Landscape, 2015).

Second, participants of the ASEAN Ministerial Conference on Cybersecurity agreed to establish an interdisciplinary institution within the framework of the ASEAN Cyber Capacity Program - ASEAN-Singapore Cybersecurity Center of Excellence (ASCCE), which will carry out expert and educational functions, as well as the functions of CERT (computer emergency response team). Within five years, it is planned to spend 30 million Singapore dollars. Australia, the USA, and Canada have already expressed their interest in participating in the activities of this Center, having proposed the implementation of their programs under its auspices (BAHARUDIN, 2018).

Finally, participants of the ASEAN Ministerial Conference on Cybersecurity endorsed a joint Singapore – UN program initiated by the Singapore Cybersecurity Agency and the UN Office for Disarmament Affairs, which includes annual seminars for representatives of ASEAN member states on cybersecurity policy planning and regulatory support [25].

SUMMARY

The national approaches of ASEAN member states in information security are determined by many factors, which affects the level of security in a specific state. However, state economies are interconnected and require harmonization of regulatory and institutional standards. At the regional level, initiatives so far cover the foreign policy aspect and consist of establishing sustainable relations, inter-agency cooperation and mutual assistance. The unification of standards will help achieve several goals: the sustainability of the digital economic system of the region, the growth of the qualitative and quantitative level of training, the increase in the investment attractiveness of the financial sector, and simplification of the procedures for creating FinTech companies. Singapore is taking the initiative in the region, however, Malaysia and Thailand are actively participating in the integration processes, so it can be assumed that the active position of most ASEAN participants will help them quickly achieve the desired results.

REFERENCES

ARF WORK PLAN ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES. Available at: http://aseanregionalforum.asean.org/wp-content/uploads/2018/07/ARF-Work-Plan-on-Security-of-and-in-the-Use-of-Information-and-Communications-Technologies.pdf. Access 08. Oct. 2020

BALUTA, T., RAMAPANTULU, L., TEO, Y. M., CHANG, E. C. *Modeling the Effects of Insider Threats on Cybersecurity of Complex Systems, Proceedings of the Winter Simulation Conference* (50th Anniversary), p. 4360-4371, IEEE Computer Society Press, Las Vegas, Nevada, US, Dec 3-6, 2017. 2017.

CARTER, W.A., CRUMPLER, W.D. Financial Sector Cybersecurity Requirements in the Asia-Pacific Region: A Report of the CSIS Technology Policy Program (April, 2019). Washington: Center for Strategic and International Studies.

CHAIRMAN'S STATEMENT OF THE 32ND ASEAN SUMMIT (Singapore, 28 April 2018). Available at: https://www.asean2018.sg/Newsroom/Press-Releases/Press-Release-Details/20180428ChairmansStatement. Access 08. Oct. 2020

CHALLA, S. Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems. *Future Generation Computer Systems*. 2018.

CNII PORTAL. Available at: https://cnii.cybersecurity.my/main/about.html. Access 08. Oct. 2020

CYBERGREEN. Available at: https://www.cybergreen.net. Access 08. Oct. 2020

CYBERSECURITY ACT, 2019. Available at: https://thainetizen.org/wp-content/uploads/2019/11/thailand-cybersecrutiy-act-2019-en.pdf. Access 08. Oct. 2020

DOBBERSTEIN, N., GERDEMANN, D., PEREIRA, G., HOE, G. *Cybersecurity in ASEAN: An Urgent Call to Action*. 2018. Available at: https://www.cisco.com/c/dam/m/en_sg/cybersecurity/cybersecurity-in-asean/files/assets/common/downloads/publication.pdf. Access 08. Oct. 2020

E-CONOMY SEA SPOTLIGHT: UNPRECEDENTED GROWTH FOR SOUTHEAST ASIA'S $50B INTERNET ECONOMY [report by Google and TEMASEK]. 2017. Available at: https://aseanup.com/southeast-asia-digital-economy-2017. Access 08. Oct. 2020

GORIAN, E. *Singapore's leadership on cybersecurity in ASEAN: intermediate results and future prospects*. The Territory of New Opportunities. The Herald of Vladivostok State University of Economics and Service, 10(3), 103-117. 2018.

GUYEN, M. 2018. *Vietnam lawmakers approve cyber law clamping down on tech firms, dissent*. Available at: https://www.reuters.com/article/us-vietnam-socialmedia/vietnam-lawmakers-approve-cyber-law-clamping-down-on-tech-firms-dissent-idUSKBN1J80AE. Access 10. Oct. 2020

HARUDIN, H. *Asean framework on cyber security in the works*. 2018. Available at: https://www.straitstimes.com/singapore/asean-framework-on-cyber-security-in-the-works. Access 08. Oct. 2020

INDONESIA. 2018. Available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/indonesia. Access 08. Oct. 2020

IWAMOTO, K. *Rise of digital economy pushes ASEAN toward policy coordination*. 2018. Available at: https://asia.nikkei.com/Politics/Rise-of-digital-economy-pushes-ASEAN-toward-policy-coordination2. Access 08. Oct. 2020

LI, Z., LIU, X., WANG, WM., BARENJI, A VATANKHAH, HUANG, GQ CKshare: secured cloud-based knowledge-sharing blockchain for injection mold redesign. *Enterprise Information Systems*, 13(1), 1-33. (2019).

MATTIOLI, R. *Methodologies for the identification of Critical Information Infrastructure assets and services: Guidelines for charting electronic data communication networks* / R. Mattioli, C. Levy-Bencheton. Heraklion:

European Union Agency for Network and Information Security (ENISA), 2014. – 43 p., p. 7. 2014.

NOOR, E. *Asean Takes a Bold Cybersecurity Step*. 2018. Available at: https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/. Access 08. Oct. 2020

RAJ, A. *Cybersecurity readiness in the ASEAN region*. 2020. Available at: https://cybersecurityasean.com/daily-news/cybersecurity-readiness-asean-region. Access 08. Oct. 2020

RAJ, A. *Fraud Continues to be the Main Cause of Cybersecurity Incidents in Malaysia*. 2020. Available at: https://cybersecurityasean.com/daily-news/fraud-continues-be-main-cause-cybersecurity-incidents-malaysia. Access 08. Oct. 2020

REPORT OF THE GROUP OF GOVERNMENTAL EXPERTS ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY, 2015. Available at: https://undocs.org/en/A/70/174. Access 08. Oct. 2020

SINGAPORE INTERNATIONAL CYBER WEEK. Highlights and Testimonials. Available at: https://www.csa.gov.sg/news/press-releases/sicw-2018---highlights-and-testimonials. Access 08. Oct. 2020

SOUTHEAST ASIA: An Evolving Cyber Threat Landscape: Special Report Singapore: FireEye Threat Intelligence, 15 p. 2015.

TER, K.L. Singapore's cybersecurity strategy. *Computer Law and Security Review*. 34(4), 924-927. 2018.

TOOMGUM, S. Thailand among top 20 nations focusing on cybersecurity. 2017. Available at: http://www.nationmultimedia.com/detail/Economy/30325029. Access 08. Oct. 2020

ZHANG, P., HE, Y., CHOW K. P. Fraud track on secure electronic check system. *International Journal of Digital Crime and Forensics,* 10(2), 137-144. 2018.

[i]School of Law. Vladivostok State University of Economics and Service. Vladivostok. E-mail: russia.ella.gorian@gmail.com. ORCID: https://orcid.org/0000-0002-5962-3929

Received: 20 Oct.2020
Approved: 01 Dec.2020