UDC 340.5

Criminalization of dangerous acts in cyberspace in criminal codes of Lithuania and Russia: comparative aspects

Stitilis Darius
Full Doctor of Law, professor,
head of the committee of the "Right of new technologies" program,
Mykolas Romeris University,
P.O. Box 08303, Ateities str., No. 20, Vilnius, Lithuania;
e-mail: stitilis@mruni.eu

Klisauskas Valdas
Assistant,
Mykolas Romeris University,
P.O. Box 08303, Ateities str., No. 20, Vilnius, Lithuania;
e-mail: v.klisauskas@gmail.com

Abstract

During the survey criminal acts of the Republic of Lithuania and Russian Federation regulating cybercrimes and responsibility for their performance as per comparative aspect.

Few different methods have been used for executation of the survey: surveying Lithuanian and Russian criminal acts for cybercrimes, comparative method has been chosen by authors. Using sources of scientific literature authors has used deductive method letting to make rather reliable conclusions. Authors of concepts for the survey have served the newest scientific literature and dictionaries.

The survey has revealed that some act for cybercrimes are criminalized differently in Lithuanian and Russian criminal acts. These differences of right reg-

ulation are being proveded and commented including possibilities of appliance of legal regulation practice of the good appropriate area as well.

Keywords

Cybercrimes, legal regulation, criminalization of dangerous acts in cyberspace.

Introduction

In XXI century having offer of information and computerized technologies under rapid improvement, having higher accessibility of the Internet including various electronic services (such as banking, Internet stores and etc.), and these technologies become rooted in all areas of human life more and more. In spite of the fact all these so called "The high technologies" have inserted lots of positive changes into human life, but is the same way has opened ways for raise of new type of crimes.

In nowadays age of technics no-one is surprised with knowledge about spread of new virus, breaking into databases, and stealth of information or execution of illegal bank transfer. As further as more cyber attacks becomes serious (Trojans, computer zombies nets and etc.), not only a wish to show own ingenuity, professional knowledge or to get financial benefit, but also political, racist or sexual abuse motives for creation of these. Electronic criminality has become global feature making more and more damage on separate citizens, organizations, whole society and state. Majority of countries of the world equalizes crimes under their dangerousness and profitability to such activities as terrorism and drug trafficking. For such reason a problem of regulation of cybercrimes in criminal acts is one of the most actual in the world, including Lithuania and our neighbor Russia.

As statistic data witnesses several thousand of cybercrimes are being executed in Russia. Paying attention on the fact that latency of cybercrimes in Russia composes 95 perc. under valuation of some experts real number of executed cybercrimes should be higher in dozen times. Furthermore, attacks from Russia against natural and legal persons located in others countries are being registered daily. Electronic criminal of this country are being mostely named as mostly

professional in the world, wisely using computers and the Internet for spying, manipulation of banking information, breaking of the Internet sites, stealth of data and sim... For this reason rather high attention on solving of the cybercrimes is being paid in Russia.

Creation of an appropriate legal basis in Russia has been started up even in the beginning of 1990 and continuous improvement of it has been under act during the few last decades. Russia separately as Lithuania has not already ratified Convention on cybercrime that are being more often criticized as ineffective, so it is important to analyze practice applied in Russia. Having analyzed similarities and differences of legal regulation of cybercrimes in the Republic of Lithuania and Russian Federation, finalization and match to rapidly improving cybercrimes of acts for cybercrimes, to identify basic problems of regulation of cybercrimes and to tender offers for support of the good Russian practice. So the results of this work could be useful for the legislator as identifying sufficient support as in criminalization of dangerous acts in cyberspace.

Novelty of the theme. Theme of regulation of cybercrimes in Lithuania has been less interesting for majority for years, but recently it is more often interesting not only for lawyers – trainees, but for scientists as well. Nevertheless, analysis of cybercrimes in Lithuanian scientific literature is rather limited. Aspect of regulation of separate types of cybercrimes have been analyzed by: D. Štitilis, M. Kiškis, I. Rotomskis, R. Petrauskas, M. Laurinaitis and so on.

In all master works written before concepts of cybercrimes, legal regulation of separate types of cybercrimes and survey of cybercrimes has been analyzed.

It is necessary to recognize that Russian authors have started to interest in cybercrimes and analysis of their legal regulation rather in advance. Problem of concept of cybercrimes, aspects of legal regulation of cybercrimes in Russia and their criminalist surveys aspects, questions of international legal basis in an area of cybercrimes have been analyzed by M.V., Dremluga R.I., Mazurov V., A. Vekhov V. B., Popova V. V., Volevodz A. G. Segro A. and so on.

Unfortunately we failed to find comparison between practices of regulation of cybercrimes in Russian Federation and in the Republic of Lithuania in sources of literature.

Subject of survey – cybercrimes.

Matter of survey – Criminal acts of Russian Federation and the Republic

of Lithuania (under comparative aspect) as much as it is concerned to cybercrimes. The matter of survey in this article is limited with narrow understanding of cybercrimes, under which dangerous acts in cyberspace having single matter are being named cybercrimes: these acts are foreseen in chapter XXX of Criminal Code of the Republic of Lithuania.

Target of the work – to analyze and compare in between regulation of cybercrimes in Russian Federation and in the Republic of Lithuania.

Exercises:

– to analyze legal norms of Criminal Codes of the Republic of Lithuania and Russian Federation for cybercrimes in comparative aspect.

– to identify problems of legal regulation of cybercrimes in Codes of the Republic of Lithuania and Russian Federation and to tender offers about possibility for solution of such problems.

Various **survey methods** have been used in the work integrated.

Documental analysis method has been used in analysis of scientific literature, legal acts and other documents, where aspects of regulation of dangerous acts in cyberspace have been included.

Legal documents analysis method together with *logical – analytic method* has been used in analyzing Lithuanian and Russian legal norms firmed in national legal acts about specialties cybercrimes releasing content of legal norms.

Comparative method has been applied for reveal of difference and communities of Lithuanian and Russian legal acts about cybercrimes also comparing national criminal legal norms to requirements of international documents. Comparative method has also been used for comparison of views of separate authors.

Generalization method has helped for tender of intermediate and final conclusions of the work and used literature has been generalized. Deduction and induction methods have already been applied in formation of conclusion of this work.

Assumptions of criminalization of dangerous acts in cyberspace in Lithuanian and Russian criminal codes

In the last decades rapid spreading of information technologies and highly increased value of computer information in social life is being observed together with increase of scale of cybercrimes. This has conditioned the legislator to take measures helping to protect

the cyberspace. One of the basic national state legislators exercises in fighting cybercrimes – forbid dangerous acts in national criminal codes[1].

Certainly, using computer/computer systems it is possible to make many criminal acts also such, when computer information is subject of a crime and such, when computer/computer system is being used as offense instrument. Paying attention on limited size of our work we will analyze in our work how cybercrimes are being understood in narrow meaning are forbidden in Lithuanian and Russian criminal codes, i.e. we will analyze that dangerous acts mentioned in separate parts of criminal acts having common subject – public relations in area of information processing only.

In 1st of May 2003, when the new criminal code of the Republic of Lithuania has entered into force (further – RL CC), system of criminal law of the Republic of Lithuania has been reformed. "A distinctive feature of new CC is that it is a modern code showing the trends and ideas of development of criminal law including wins of science of this area of law".[2] XXX chapter has been excluded in this code "Crimes against informatics" that has been renamed into "Crimes against security of electronic data and information systems" in 2007.

We can set what values are being to be secured by the legislator by using a way offered by the doctrine of criminal law, for namely "values secured by criminal act is basic criteria of breakdown Criminal code special part norms into sections" Therefore, firstly, attention should be paid on the name of an appropriate RL CC chapter – "Crimes against security of electronic data and information systems". Obviously, it is aimed to secure electronic data and information systems with this chapter; furthermore, it is encroached on common subject – public relations in area of information processing by using all criminal acts mentioned in this chapter of RL CC.

RL CC XXX chapter "Crimes against security of electronic data and information systems"[3] is composed of 5 articles stating criminal liability for all criminal acts:

1 Stitilis, D. (2011), *Cybercrimes. Methodic measure*, Mykolas Romeris university, Vilnius, p. 84.

2 Piesliakas, V. (2006), *Lithuanian criminal law. The first book*, Justitia, Vilnius, p. 63.

3 "Criminal code of the Republic of Lithuania", *Official Gazette*, 2000, No. 89-2741; "Criminal code of the Republic of Lithuania", *Official Gazette*, 2004, No. 25-760; "Criminal code of the Republic of Lithuania", *Official Gazette*, 2007, No. 81-3309.

– Unlawful access and influence on electronic data incurring major damage (196 art.);

– Unlawful influence on an information system incurring major damage (197 art.);

– Unlawful interception and use of electronic data (198 art.);

– Unlawful Access to an Information System by damaging the protection of measures of the information system (1981 art.);

– Unlawful Disposal of Installations, Software, Passwords, Login Codes and Other Data directly intended for the commission of criminal acts (1982 art.).

Setting of criminal liability for cybercrimes is not an exclusive attribute of criminal law of the Republic of Lithuania. Chapter criminalizing these acts is formed in criminal code of Russian Federation also (further – RF CC). In 1st of January 1997, when Russian Federation criminal code has entered into force, 28 chapter "Crimes in area of computer information" is excluded. We can make a conclusion from the name of the chapter that criminal acts encroaching common subject – public relation in area of computer information processing are being excluded.

RF CC 28 chapter "Crimes in area of computer information " is composed of 3 articles that has been essentially changed in the end of 2011 and stated in new redactions after an acting Russian Federal Act no. 520-FZ "For change of Criminal Code of Russian Federation and separate legal acts of Russian Federation"[4] dated 7th of December 2011. Criminal liability in these 3 articles is set for these criminal acts:

– Unlawful access to computer information (272 art.);

– Creation, usage or distribution of malicious programs (273 art.);

– Breach of regulations of security, processing or transmission of computer information and information-telecomunication networks (274 art.).

In concept of analyzed theme legal norms stated in mentioned chapter of criminal code are actual under the aspect that analysis of criminal legal norms is important willing to reveal common situation of regulation of cybercrime in a state, for, exactly, sufficient criminal regulation is one of assumptions able to

4 "Federal law of the Russian Federation on 7 December 2011 No. 420-FZ "On amending the Criminal code of the Russian Federation and separate legislative acts of the Russian Federation" ["Federal'nyi zakon Rossiiskoi Federatsii ot 7 dekabrya 2011 g. N 420-FZ "O vnesenii izmenenii v Ugolovnyi kodeks Rossiiskoi Federatsii i otdel'nye zakonodatel'nye akty Rossiiskoi Federatsii"], available at: www.rg.ru/2011/12/08/p-raboty-site-dok.html

decrease number of cybercrimes. Reaching to reveal similarities and differences of practice of regulation of cybercrimes used in criminal acts in Lithuania and Russia, also marking possible gaps of regulation, we will analyze legal norms for cybercrimes of criminal codes of the Republic of Lithuania and Russian Federation under comparative aspect. We will make this comparative analysis on the basis of analysis of content of separate attributes of composition of criminal act paying more attention on question of composition of attributes of criminal act that causes discussions.

Criminal liability for unlawful access to electronic data and influence on this

Criminal liability for unlawful access to electronic data and influence on this data in Lithuania can rise under RL CC 196 art. "Unlawful influence on electronic data".

Criminal liability foreseen in RL CC 196 art. 1 p. for destruction, damage, removal or modification of electronic data or a technical equipment, software or otherwise restricts the use of such data thereby incurring major damage, and 2p. of this article foreseen criminal liability for the same act in respect of the electronic data of an information system of strategic importance for national security or of major importance for state government, the economy or the financial system.

Basic subject of this criminal act – security of electronic data.

Subject of criminal act foreseen in 1p. of this article – any electronic data, and in 2. p of this article – electronic data of an information system of strategic importance for national security or of major importance for state government, the economy or the financial system only. In 2 article of Act on an electronic signature electronic data is described as all data managed using measures of information technologies[5].

RL CC 196 art. Objective side of foreseen criminal act can manifest by one of few of these alternative acts:

– unlawful destruction of electronic data;

– unlawful damage of electronic data;

– unlawful removal of electronic data;

– unlawful modification of electronic data;

5 "Law of the Republic of Lithuania on electronic signature", *Official Gazette*, 2000, No. 61-1827, Art. 2.

– technical equipment, software or otherwise restricts the use of such data.

Having executed these alternative criminal acts (-s) for letting qualify as finished criminal act these three conditions are necessary to be executed:

1. These acts must be unlawful. *It means that person executing such acts is not lawful user of electronic data – has no legal permission of the owner or possessor of electronic data to use or work with detailed information, or such usage or work with electronic data is forbidden by other legal acts (egz., Act of state and official secrets foresees that classified information can be entrusted for persons having appropriate permissions to work or get acquainted with classified information only). Unlawfulness will also be in case, when person is provided with a limited right to use or work with data (egz. To get acquainted, to amend only), but he overcoming his competence (authorities given) makes acts under which these data is being destructed, damaged, removed or modified*[6].

2. Real damage must raise – data or limited usage of these must be destroyed, damaged, removed or modified and in all cases this damage must be major.

3. Exactly for these acts of offending person (and not for egz. a mistake of software and sim.) The injured must feel major damage, i.e. there must be causality between processed acts and consequences raised.

It should be noted that legislator has not tendered a clarification what damage is named as major[7]. In such case court leaves a right to decide in any concrete case is the made damage major, actually, common principles of setting major damage and its valuation criteria should be formed by practice of courts.

Panevėžys town district court analyzing criminal case No. 1-187-389/2011 has set that R. Š. had modified electronic data located in computer unlawfully and had wasted alien assets of JSC "D" entrusted to him–2,000 liters of diesel of total value 5,957.40 Lt by transferring it to undetermined persons so making major damage to JSC "Deliuvis"."[8] Furthermore, in this case court has stated that damage of value 5,957.40 Lt can already be named as major and criminal act is being qualified under RL CC 196 art. 1 p.

6 *Comment of criminal code of the Republic of Lithuania. Special part. II volume*, Registrų centras, Vilnius, 2009, p. 419.

7 While, such damage is observed further in RF CC.

8 Panevėžys town district court, decision 25th of October 2011 in criminal case No. 1-187-389/2011.

Whereas, Vilnius town 2nd district court analyzing criminal case, in which V. Č. accused unlawfully succeeded, converted and stored non-public electronic data; unlawfully acquired and stored passwords, logins directly designed for making criminal acts; having unlawfully accessed to information system, breaking security measures of information system; having unlawfully modified electronic data, making minor damage, has stated, that having made two unlawful acts of modifying electronic data had made to SI(data not for publication) college totally minor damage of value 5,000 Litas damage.[9] We can see from example of this case that under opinion of other court 5,000 Lt damage is being named as major. Furthermore, it is evident that having no clearly defined criteria divide between major and minor damage is being set very difficult and refers on individual valuation of each court.

Kaunas town district court analyzing criminal case, in which A. A., citizen of the Republic of Lithuania, having education of 11 grades, single, and scholarship of Kaunas secondary school has been accused making criminal acts foreseen in criminal code of the Republic of Lithuania 196 art. 1 p. and 196 art. 2p. has stated that "accused had made major damage (it is not defined with material size) mentioned in disposition of Code 196 art. 1p.: it can be seen from clarifications of representatives of civil plaintiff that destroyed site had been created in 2004, it had contained a lot of information, to restore which no possibility exists."[10]In this case representatives of civil plaintiff rather evidently grounded the damage, stating that: *"After break-in (data not for publication) into site of secondary school, it has been totally destroyed unrecoverable, for the tender of the site renews changes made in the site on Fridays having not stored previous data. Site (data not for publication) had been created in 2004, lots of data had been inserted into the site, near to 1,000 photo pictures and other information about the school, this data had been destroyed unrecoverable, these are to collect again, so after destruction of the site major damage has been done to the school. The school had always participated in competitions of scholar sites, had won these not for once. Creation of new site has cost 10,000 Lt, but it has not been already paid: it has been agreed*

9 Vilnius town 2 district court, decision dated 27th of May 2009 in criminal case No. 1-515-487/2009.

10 Kaunas town district court, decision dated 25th of October 2011 in criminal case No.1-2092-246/2011.

Table 1. Cases received and analyzed in I instance courts under 196 art. during 2007-2011

Year	Balance of unfinished cases in the beginning of reporting period	Cases received	Cases finished	Balance of unfinished cases in the end of reporting period	Duration of proceedings		
					Up to 6 months	From 6 up to 12 months	12 months and longer
2011	1	0	1	0	0	1	0
2010	0	1	0	1	0	0	0
2009	2	1	3	0	2	0	1
2008	0	2	0	2	0	0	0
2007	0	0	0	0	0	0	0

Source: Statistics of courts http://www.teismai.lt/lt/teismai/teismai-statistika

with JSC "(data not for publication)", having performed reconstruction of the site that invoice of 10,000 Lt will be paid until 01-12-2011."[11]

Obviously, that under practice of courts major damage made can be both pecuniary and non-pecuniary (moral, social and sim.).

Nevertheless, ways of destruction, damage, removal and modification of electronic data are not foreseen in this composition.

Speaking about subjective side of such article it is required to notify that form of guiltiness can be intentionally – both direct and indirect only.

Subject under RL CC 196 art. can be a natural person of diminished capacity elder than 16, also legal person.

Following alternative punishments are foreseen in the sanction for unlawful influence on electronic data – community service or by a fine or by imprisonment for a term of up to four years; for unlawful influence on data of an information system of strategic importance for national security or of major importance for state government, the economy or the financial system – a fine or by arrest or by imprisonment for a term of up to six years.

According to CC 11 art. 4 part, criminal cases where criminal liability is foreseen under 196 art., attributable to group of less serious crime.

For the reason legislator has not provided clarification of concepts used in 196 art., has already set alternative sanctions can be applicable for criminal act foreseen in the article, practice of courts has major influence on how this article

11 Kaunas town district court, decision dated 25th of October 2011 in criminal case No.1-2092-246/2011.

is being relised in real life . For this reason a table showing statistics about received and analyzed cases under 196 art. in courts of I instance during the last five years i.e. 2007-2011 is being given.

As one can see from statistics of cases analyzed in courts very less of cases under this article reaches the court, the biggest "rush" has been in 2008, when the court has received "even" two cases. Doubly enough that just one or two acts of such type are being done during the year, so maybe, reasons should be searched somewhere else. Under our opinion, few assumptions can be made, why cases under this article are not reaching the court. One of these – high latency of such criminal acts. Other – investigators making pretrial investigation is hard to prove that major damage has been made, especially, if non-pecuniary type has stated no clear criteria of such "major" damage valuation. Notable, that practice of courts analyzing cases of such type is just under formation, so evidently, long enough period will have to pass while common understanding of concepts undefined in disposition (egz. major damage) of 196 art. is formed.

Under our opinion it would be still appropriate to amend XXX chapter with one more article, where clarification of very abstract concept "major damage" is provided revealing both pecuniary and non-pecuniary aspects of the concept. The problem of different treatment of this concept would be avoided together with problem of qualifying. Especially, that such practice to provide clarifications of the concept in the same RL CC are being executed, egz. RL CC 190 art. value of property is clarified as being applied for crimes of XXVIII chapter.

In Russia criminal liability for unlawful access to computer information caused negative influence on this information is foreseen under RF CC 272 art. "Unlawful access to computer information"

Notable, that column "Notes" is being added to RF CC 272 art. where clarification of few used concepts is being provided. Here it is specified that computer information is being understood as information (messages, data) provided using support of electronic signals, independently from way of its storage, processing or transfer.

In RF CC 272 art. 1 p. criminal liability for unlawful access to computer information secured by the legal act, if this has caused destruction, blocking, modification or copying, of computer information, and 2p. criminal liability for the same act causing major damage or made from selfish motives is foreseen. In

this article 3 p. criminal liability for the same acts foreseen in points 1 and 2 of this article is foreseen, in case these acts are made by the group of persons agreed in advance, or organized group or by the a person taking advantage of its official position, and in 4p. of this article criminal act for the same activities as foreseen in point 1, 2 and 3 of this article is foreseen, in case these caused serious consequences or composed conditions for their appearance.

Subject of this criminal act – security of information saved by the act essentially matches RL CC 196 art. Foreseen subject of criminal act – security of electronic data.

A common matter of RF CC 272 art. – computer information secured by the act. For the meaning, what is information "secured by the act "opinions of Russian scientists differ. Part of authors clarify this meaning rather narrow as, for instance, M.M. Karelina, that shows that information secured by the act means such information security for that is set by special acts (state, professional and commercial secrets, personal data and etc.)[12]. Whereas, other part of authors clarifies this concept wider, for instance, Y. V. Gavril in, revealing content of this concept he grounds with Constitution, Civil code of Russian Federation and other legal acts and he shows that secured by the law information can be of natural and juridical persons, as well as state information.[13]. We would approve the opinion of the latter author, for the assumption that legislator had a wish to secure all the information, but not just a part of it is more probable. Furthermore, in case we would interpret this concept extensively, so the subject of the crime is mostly similar to the object of RL CC 196 art.

In RF CC 272 art. foreseen objective side of the crime can be defined as unlawful access to computer information secured by the act, if this has caused destruction, blocking, modification or copying of the computer information. Under our opinion, objective side of this crime has many similarities to objective side of RL CC 196 art. That includes the same acts as destruction, blocking and modification of electronic data, exclud-

12 Karelina, M.M., "Crimes in the sphere of computer information" ["Prestupleniya v sfere komp'yuternoi informatsii"], available at: www.crime-research.ru/library/CodeRu.htm

13 Gavrilin, Yu.V. (2003), *Crimes in the sphere of computer information. Qualification and evidence: study guide* [*Prestupleniya v sfere komp'yuternoi informatsii: kvalifikatsiya i dokazyvanie: Ucheb. posobie*], YuI MVD RF, Moscow, p. 16.

ing the one – copying of electronic data. Whereas, criminal liability for copying of non-public electronic data as foreseen in other RL CC article – 198 that will be more detailed analyzed by us in our work later.

We can see from disposition of RF CC 272 article that act of such type is being named as criminal, in case four essential conditions are being executeed realizing it:

1. access to computer information must be unlawful (essentially, the same condition is foreseen in RL CC 196 art.);

2. encroaching not at any computer information, but at such as secured by the act;

3. negative consequences must raise – destruction, blocking, modification or copying of the computer information;

4. exactly for this act of offending person (but not for egz. error of software and sim.) computer information has been destroyed, blocked, modified or copied, i.e. causality between actions made no consequences raised must be set (the same is demanded by RL CC 196 art. disposition). "..simple match of time of unlawful access and break of computer system or error of software does not impose criminal liability".[14]

The fact that an appropriate act can not be named as criminal in case one of these four attributes as per RF CC 272 art. is also confirmed by practice of courts of Russia. Court of autonomic region Yamal-Nenets has stated by the cassation decision dated 16th of February 2012 that: "*ground for conviction of K. has been such that during the period from 30th of March 2011 till 5th of June he reaching unlawful access to the Internet network had used registration data of other users (user name and password), having entered these into setting of his computer. For this reason names of subscribers, number of their personal accounts, information about flows of data, payments of invoices, registration data (user names and passwords) had been rewritten into memory of his computer's hard disc. Necessary attribute of the crime foreseen in 272 art. 1 p. is named consequences, such as destruction, blocking, copying and modification of computer information. Furthermore, such consequences must be result of unlawful access to computer information secured by the act, i.e. causality must rise between them. Moreover, court has stated in the descriptive-grounds of de-*

14 Naumov, V., "National legislation in the fight against computer crime" ["Otechestvennoe zakonodatel'stvo v bor'be s komp'yuternymi prestupleniyami"], available at: www.hackzone.ru/articles/a5.html

cision just the fact of unlawful rewriting of computer information into hard disc of personal computer of the accused. It has not been named in the descriptive-grounds of decision that some consequences had raised for activities made by K. As foreseen in 272 art. 1 p. For this reason, town's decision has been denied under cassation decision dated 16th of February 2012, the criminal case has been returned for the trial reset. "15

As many discussion about what access to computer information is to be named as unlawful in the scientific literature, we will discuss this concept wider. Y. Gulbin thinks that unlawful access to information is such an access, when valid legal norms, administrative acts regulating access of information between persons (group of persons) are being breached".[16] Under our opinion unlawful access should not be related with breach of norm legal acts, for than it comes out unclear how we should state the same access to data that is not regulated by norm acts, but when the owner of this date had not gave a permission to access to this data. T.I. Vaulina thinks that unlawful access should be named as access to the closed information system that is executed by a person being unlawful owner of this information or having no permission to work with this information".[17] But his description raises a lot of additional question – it is not clear, what is "closed information system". Under opinion of V. Naumov, "Access to computer information secured by the act is can be named as unlawful, if it is being done by a person having no right to get this information and work with it (including computer system)".[18] O M.M. Karelina also remarks that "such information should also be applied with security measures by stating persons that are able to access it."[19] We would approve

15 "Actual cassation decisions in criminal cases during period 11th – 20th of February 2012" ["Aktual'nye kassatsionnye opredeleniya po ugolovnym delam za period s 11 po 20 fevralya 2012 goda"], available at: http://oblsud.ynao.sudrf.ru/modules.php?name=press_dep&op=1&did=538

16 Gul'bin, Yu., "Crimes in the sphere of computer information" ["Prestupleniya v sfere komp'yuternoi informatsii"], available at: www.lawmix.ru/comm/8288/

17 Vetrov, N.I., Lyapunov, Yu.I. (1998), *Criminal law. Special part* [*Ugolovnoe pravo. Osobennaya chast'*], Yurisprudentsiya, Moscow, p.557.

18 Naumov, V., "National legislation in the fight against computer crime" ["Otechestvennoe zakonodatel'stvo v bor'be s komp'yuternymi prestupleniyami"], available at: www.hackzone.ru/articles/a5.html

19 Karelina, M.M., "Crimes in the sphere of computer information" ["Prestupleniya v sfere komp'yuternoi informatsii"],

this joint description composed of two authors' opinions.

There, court of Dzerzhinsky town having analyzed case of unlawful access to computer information has set that Galushkin D.A., during the period from 10th of December 2010 till 4th of October 2010 had worked in OOO TK and he had been provided for the execution of professional duties (a topic correspondence) with the password to connect post box of the company. Galushkin D.A. had been retired on 4th of October 2010 from his duties and understanding that mentioned password for connecting post box of the company had been provided him excluding for working purposes and that it does not belong to him after he becomes retired and he has no right to use the post box of the company, he has connected it for criminal targets. Court has stated that Galushkin D.A. had executed unlawful access to computer information, for he connected post box of the company unlawfully, i.e. having no permission of the owner of computer information OOO TK. Furthermore, Galushkin D.A. had destroyed the password of access to the post box, that had been set by the owner SC TK and had blocked possibility to connect to the own post box.[20] Thus, in this case court has also stated that access is being named as unlawful having no permission of the owner of information and breaching security measures set by the owner.

In 272 art. 2, 3 and 4 parts aggravating circumstances for these the crime is being called as more serious are being foreseen as a circumstance of what more strict sanctions are being foreseen and these are concerned by the legislator with:

– Subject of the crime:

– criminal act is being made by the group of persons agreed in advance;

– criminal act is being made by the organized group; Attention should be paid on that under RL CC 60 art. in case criminal act is being made by accomplices or organized group, it is always being called as aggravating circumstance by sentencing, independent on the type of criminal act is being made.

– criminal act is being made by a person taking advantage of his official position.

– Subjective side of the crime:

available at: www.crime-research.ru/library/CodeRu.htm

20 "The Decision of Dzerzhinsky town court dated 27th of July 2011 Case No (not defined)" ["Delo No. (ne opredeleno) Prigovor imenem Rossiiskoi Federatsii, g. Dzerzhinsk 27 iyulya 2011 goda"], available at: www.gcourts.ru/case/1446171

– criminal act is being made out of selfish wishes.

– Consequences of the crime:

– criminal act has caused major damage. In the notes provided to RFCC 272 art. Definition of major damages given by showing that major damage foreseen in this article is such with value overcoming one Million of Rubbles. Whereas in RL CC 196 art. Condition that criminal act must cause major act is not an aggravating circumstance, but necessary condition for criminal act under this article to rise.

– criminal act has caused serious consequences or made conditions for them to rise. Meaning of concept "serious a circumstance" has not been given in RF CC, so court is to solve are serious consequences caused in each concrete case.

Whereas, RL CC 196 art. circumstances aggravating the crime is concerned to the subject of the crime only i.e. in case of assassination on electronic data of an information system of strategic importance for national security or of major importance for state government, the economy or the financial system. Russian legislator has not excluded value of the subject as qualifying attribute, what, in our opinion, can be stated as legal gap. We have an idea that information on that assessation is being done is not of equivalent and more strict liability should be foreseen for an association on information mostly important for functionality and security of the whole state really than on information belonging to one natural person.

Notable, that reading scientific literature and analyzing practice of courts one can more often note that cybercrimes are being made by employees taking advantage of the official position and making damage exactly for the entity, bank or other institution they are working in.

For instance, Panevėžys town district court analyzing criminal case No. 1-187-389/2011, has stated that *R. Š. working as manager and being responsible for UAB "D" fuel station No. 3 material and monetary Balances, they movement and composition of reports during the period from 12th of December 2007till 1st of February 2008 for not showing lack of 2,000 liters of diesel in the reports filled for the end of the month, had unlawful modified electronic data located in computer, it means, has amended an information system with new non-existing electronic data, namely: on 12th of December 2007 under the consignment note No. 0002393 had entered into computer system13,293 litters of diesel delivered to fuel station No. 3 at*

12:40:05 hrs., after that she formed non-existing document No. 00001 at 09:13:54 hrs., using that she had deducted 3,000 liters of diesel from the program, on 14th of December 2007, at 15:29:46 val., she had formed non-existing document DID No. Nr. 1111, using that she had inserted 1,000 liters of diesel into the program, on 31st of December 2007, at 23:25:02 hrs. she had formed non-existing document No 00000345, using that she had entered 2,000 liters of diesel into the program, on 1st of January 2008, at 01:31:35 hrs. she had formed non-existing document No. 00000345, using that she had deducted 2,000 liters of diesel form the program, on 31st of January 2008, at 20:43:38 hrs., she had formed non-existing document No. 002, using that she had inserted 2,000 litters of diesel into the program, on 1st of February 2008 at 06:09:29 hrs., she had formed non-existing document No.01/002, using that she had deducted 2,000 litters of diesel from the program and in such way she had wasted alien property entrusted to her belonging to JSC"D"–2,000 litters of diesel for total value of 5,957.40 L by transferring it to undetermined persons in such way making major damage for JSC ,,Deliuvis".[21]

From this case we can see that person having made criminal act is in concern with the company in labor relations. In case perpetrator having used advantage of professional position for criminal targets match attribute of special subject – he is public officer or equivalent person, in this case question of qualification of perpetrator's acts under RL CC 228 article "**Abuse of Office**"(1 p. – "A civil servant or a person equivalent thereto who abuses his official position or exceeds his powers, where this incurs major damage to the State, an international public organization, a legal or natural person <...>. 2 p. A person who commits the act provided for in paragraph 1 of this Article seeking material or another personal gain, in the absence of characteristics of bribery <...>[22]). However, in the case provided above perpetrator had been in concern with the employer in labor relations grounded with labor treatment, so her abuse of official position can not be incriminated under match with RL CC 228 article.

Considering that more cybercrimes are being made by employees us-

21 Panevėžys town district court, decision 25th of October 2011 in criminal case No. 1-187-389/2011

22 "Criminal code of the Republic of Lithuania", *Official Gazette*, 2000, No. 89-2741; "Criminal code of the Republic of Lithuania", *Official Gazette*, 2004, No. 25-760; Criminal code of the Republic of Lithuania", *Official Gazette*, 2007, No. 81-3309.

ing advantage of their duties they take, also the fact that such persons that have access to important electronic documents for duties they take can often make more greater damage for an appropriate institution than other persons, we would thing that it would be appropriate to set additional qualifying attribute in RL CC 196 art. (as it has been done in RF CC 272 art.) – in case criminal act is being made by the person using its advantage of official position. Under our opinion in this case setting of more strict punishment could act preventively reaching decrease cases, when "company/entity is being damaged from inside".

RF CC 272 art. subjective side of foreseen criminal act – direct intention, while in RL CC 196 art. For guilt can be both direct and indirect intention.

RF CC 272 art. does not regulate a situation, when unlawful access is being made for carelessness, for this liability is not increasing for majority of acts even those that has been really done under intention.[23]

In RF CC 272 art. subject of foreseen criminal act – natural person of diminished capacity and legal age. Separately than in RL CC 196 art., RF CC 272 art. has not set that juridical persons are being prosecuted. In such a case, if unlawful act is being made by representative of juridical person, so liability some directly on this natural person.

In sanction of RF CC 272 art. 1 p. these alternative punishments are set – penalty up to two thousands Rubles or size of salary received, or other revenues of sentenced received in the period of eighteen months, or correctional labor for a term of up to one year, or restriction of liberty for a term of up to two years or imprisonment for the same term. Comparing sanctions for the basic composition of criminal act, one can see that in RL CC 196 art. double stronger imprisonment punishment is foreseen.

In RF CC 272 art. 2 p. – penalty from one hundred thousand up to three hundred thousand Rubles or size of salary received, other revenues of sentenced received in the period from one for a term of up to two years, or correctional labor for a term of from one up to two years, or restriction of liberty up to four years, or forced labor for a term of up to four years, or arrest for a term of up to six months, or imprisonment for the same term. RF CC 272 art. 3 p. – penalty up to five thousand Rubles or size of salary received, or other

23 Naumov, V., "National legislation in the fight against computer crime" ["Otechestvennoe zakonodatel'stvo v bor'be s komp'yuternymi prestupleniyami"], available at: www.hackzone.ru/articles/a5.html

revenues of sentenced received in the period of three years together with foreclosure to take appropriate duties or making certain act up to three years, or restriction of liberty for a term of up to four years, or forced labor up to five years, or imprisonment for the same term. RF CC 272 art. 4 p. – an imprisonment for a term of up to seven years.

Comparing sanctions for these qualified compositions of the crime with sanctions for qualified compositions of the crime foreseen in RL CC 196 art. we see different than in an appropriate RL CC art. possibility of "double punishments "is foreseen (egz. penalty together with foreclosure to take appropriate duties or making certain act). Sanctions in articles are being compared do not differ essentially by their size, but for the most dangerous criminal act foreseen in RF CC 272 art. imprisonment punishment can be intended only.

Having analyzed that having made criminal act set in RL CC 196 art. 2 p. damage is being made for such essential state interests as public security, state government, financial interests and other, we think that it should not be tolerated and for making it punishment should be strict. Under our opinion alternative sanction – penalty foreseen in RL CC 196 art. 2 p. is too soft and inadequate to the crime is being made, while RF CC 272 art. 4 p. has a foreseen sanction as more deterrent. Considering on stipulated we would offer to deny a possibility for intending a penalty in a sanction of RL CC 196 art. 2 p..

According to RF CC 15 art. 2 p. criminal acts, for which criminal liability under 272 art. 1 p. is foreseen are deriven to group of mild crimes, and according to RF CC 15 art. 3 p., criminal acts, for which criminal liability under 272 art. 2 p. is foreseen are deriven to group of less serious crimes.

Furthermore, attention should be paid on, actually, a mistake of correction has been made RF CC 272 art. 2 p. for it looks very strange that for a crime made under aggravating circumstances imprisonment up to 6 months can be intended, whereas, for the basic composition of the crime – up to two years.

Summarizing an above, in our opinion RF CC 272 art. with its nature is more similar o RL CC 196 art.

Unfortunately, according to the fact that modifications of RF CC 272 art. have been done just few months ago, we are not able to provide statistics for comparison how many cases have been analyzed I instance courts in Russia during the last five years, i.e. 2007 – 2011 under the same article.

Criminal liability for unlawful interception

Criminal liability for unlawful interception of electronic data in Lithuania can rise under RL CC 198 art. "Unlawful interception and use of electronic data".

In RL CC 198 art. 1 p. criminal liability for unlawful observation, record, interception, acquisition, storage, appropriation, distribution or otherwise use of the electronic data which may not be made public is foreseen, and in RL CC 198 art. 2 p. Criminal liability for unlawful observation, record, interception, acquisition, storage, appropriation, distribution or otherwise use of the electronic data which may not be made public and which are of strategic importance for national security or of major importance for state government, the economy or the financial system is foreseen. Object of this criminal act – confidentiality of non-public data, and the common thing – non-public electronic data. Vilnius district court criminal division judge panel having analyzed in appeal order a criminal case under appeal claims of the convict T. S. and Vilnius town district prosecution office prosecutor for decision of Vilnius town 2nd district court dated 1st of July 2011 has marked that electronic data are being "named "as data being ordered using devices of information technologies and are created in an electronic form or replaced into such form. Electronic data is also named as a sequence of characters for transmittance of information using information technologies."[24]

Whereas, non-public data is such data that is intended not for everyone and is not being used in public. Acquisition and use of such non-public data concerning to certain limitations using special requirements or procedures that can be setting acts or other legal acts, internal documents of companies, entities and organizations, also in a case, when a person expects their private transmission[25].

In RL CC 198 art. Objective side of foreseen criminal act can manifest in one or few of these alternative acts:

– unlawful observation of non-public electronic data;

– unlawful record of non-public electronic data;

– unlawful interception of non-public electronic data;

– unlawful acquisition of non-public electronic data;

24 Vilnius district court, decision dated 23rd of December 2011 in criminal case No. 1A-977/2011.

25 *Comment of criminal code of the Republic of Lithuania. Special part. II volume*, Registrų centras, Vilnius, 2009, p. 430.

– unlawful storage of non-public electronic data;

– unlawful appropriation of non-public electronic data;

– unlawful distribution of non-public electronic data;

– unlawful otherwise usage of non-public electronic data.

Vilnius district court having analyzed a criminal case under appeal claims of the convict T. S. and Vilnius town district prosecution office prosecutor for decision of Vilnius town 2nd district court dated 1st of July 2011 has marked that "otherwise usage of electronic data is an adjustment of such data and usage of this for some other purpose. This can be for satisfaction of rowdy, selfish or other interests both of perpetrator and other persons. Objective attributes of unlawful interception and usage of electronic data is formed as alternative in disposition of the act, or it is enough for rise of neither criminal liability to make nor one of these acts."[26]

Having executed these alternative criminal act (-s) for letting qualify as finished criminal act these two conditions are necessary to be executed:

1. These acts must be unlawful; Vilnius district court criminal division judge panel having analyzed in appeal order a criminal case mentioned before has stated that *essential circumstance making acts of T. S. criminal – interception of electronic data having no right to do this. It has been set in the case that T. S., having no lawful permission of the possessor of data of electronic banking accounts generator – JSC "VSG " (data has been changed), i.e. had arbitrary and unlawfully connected using data of generator to JSC "VSG" (data has been changed) account for satisfaction of selfish interests and had made transfers of monetary funds from this account to his account and account of the company he had been leading, i.e. in the analyzed case the objective side of usage of electronic data by using generator of codes with support of what funds had been transferred into T. S. account. In such a case conclusion of the first instance court that "T. S. had not made an act foreseen in RL CC 198 art. 1 p. attributes* "is *unreasonable and inconsistent with the real factic circumstances.*[27]

2. There must be assassination on not any electronic data but only to such that is non-public, i.e. are not for use in public.

26 Vilnius district court, decision dated 23rd of December 2011 in criminal case No. 1A-977/2011.

27 Vilnius district court, decision dated 23rd of December 2011 in criminal case No. 1A-977/2011.

Table 2. Cases received and analyzed in I instance courts under 198 art. during 2007-2011

Year	Balance of unfinished cases in the beginning of reporting period	Cases received	Cases finished	Balance of unfinished cases in the end of reporting period	Duration of proceedings		
					Up to 6 months	From 6 up to 12 months	12 months and longer
2011	1	5	5	1	4	1	0
2010	0	5	4	1	4	0	0
2009	0	5	5	0	5	0	0
2008	0	3	2	1	2	0	0
2007	0	3	2	1	2	0	0

Source: Statistics of courts http://www.teismai.lt/lt/teismai/teismai-statistika

Attention should be paid on that for stating finalization of criminal act under 198 art., major damage is not necessary to be caused and causality between act and negative consequences is not necessary as it has been demanded in the article discussed before – it is enough to make act (-s) mentioned in the disposition of the article.

Speaking about subjective side of such criminal act it is required to be remarked that form of guiltiness can be direct intention only.

Subject of this criminal case – person, whose age has been sixteen before making the crime. Such person also must be of diminished capacity. Moreover, juridical person is also liable for these crimes as under RL CC 20 art. has set conditions of criminal liability of juridical persons.

Criminal acts, for which liability is foreseen under 198 art., are deriven to group of less serious crimes under CC 11 art. 4 part.

In sanction of RL CC 198 1p. these punishments are foreseen alternatively – a fine or by imprisonment for a term of up to four years; RL CC 198 art. 2 p. the only possible punishment foreseen – imprisonment for a term of up to six years.

Having analyzed table 2 provided below and compared with other provided in the work, we see that this is one of the most often articles foreseeing liability for cybercrimes, under which cases reach the court.

No separate article is excluded in Russian CC foreseeing liability for conscious and unlawful transmission of non-public electronic data into computer sys-

tem, out of it or inside it. Criminal liability for unlawful access to computer information secured by the act, in case it has cause copying of computer information only in RF CC 272 art. we have already analyzed. It is specified in the special literature that two views exist between Russian scientists, what means copying of computer information. Supporters of the first (narrower) view keep an idea that copying – interception of computer information out of one computer into another or into some other medium (egz. copying to floppy).Supporters of the second (wider) view keep an idea that copying – interception of information out of electronic storage device into any other (egz. rewriting, making photography and sim.).[28] We would approve supporters of the first view, for in our opinion wider spectrum of criminal acts then cybercrimes is being taking in under the second view.

Criminal liability for unlawful connection to information systems and influence on these

Criminal liability for unlawful connection to information systems in Lithuania is foreseen in RL CC 198(1) art. "Unlawful connection to an information system".

In RL CC 198(1) art. 1 p. criminal liability for unlawful connection to an information system by breaking devices of information systems security is foreseen, in RL CC 198(1) art. 2 p. criminal liability for unlawful connection to an information system of strategic importance for national security or of major importance for state government, the economy or the financial system is foreseen.

The basic object of unlawful connection to information systems is security (confidentiality) of information systems and data located in these, and the thing is an information system.

Objective side of crime foreseen in RL CC 198(1) art. can be described as unlawful connection to an information system by breaking security devices of an information system.

As one can see from disposition of the article act of such type is being named as dangerous, in case two main conditions are being realized during its execution:

1. connection to an information system is being done unlawfully, i.e. having no permission to make such acts from the owner or legal possessor of the information system;

28 Mazurov, V.A. (2002), *Computer crime: classification and methods of countering* [*Komp'yuternye prestupleniya: klassifikatsiya i sposoby protivodeistviya*], Logos, Moscow, p.107.

2. criminal act is being done not just simply, but in detail way mentioned in disposition of the article – connection to an information system by breaking security devices of an information system.

The fact these to essential circumstances must occur is also confirmed by practice of the courts. Vilnius town 1st district court has stated that it is fully proved that T.Č. had made criminal act foreseen in RL CC 198 art. 1 p., for "*T.Č. during the period from 13thof October 2010 till 8th of December 2011 in accommodations of SC SEB bankas through computer "DELL OptiPlex 745"located in his workplace having had set using undetermined software and later (on time set during pretrial proceedings) had changed selfish administrator's password for connection to non-public information system that had been being administrated in office accommodations of SC SEB bankas, on 13thof April 2011 at 12hrs. 01min. Unlawfully, i.e. having had no permission of owner or legal possessor of this information system to connect this information system, intentionally, breaking security devices of this system, had connected to this bank information system as a user having unlimited right of access*."[29]

29 Vilnius town 1st district court, decision dated 6th of December 2011 in criminal case No. 1-1430-276/2011

Speaking about subjective side of such criminal act, it is required to mark, that form of guiltiness can be direct intent only. Person realizes that he connects information system by breaking its security devices unlawfully and wishes to do so.

Subject of such criminal act – person of diminished capacity, whose age has been sixteen before making the crime. Moreover, juridical person is also liable for these crimes as under RL CC 20 art. has set conditions of criminal liability of juridical persons.

Criminal acts, for which liability is foreseen under 1981 art. are deriven to group of mild crimes under leadership of CC 11 art. 3 part.

In sanction of RL CC 198(1) art. 1 p. It is foreseen that these alternative punishments can be intended for unlawful connection to as information system: community service or by a fine or by arrest or by imprisonment for a term of up to one year; and in sanction of RL CC 198(1) art. 2 p. It is foreseen that for unlawful connection to an information system of strategic importance for national security or of major importance for state government, the economy or the financial system – a fine or by arrest or by imprisonment for a term of up to three years.

Table 3. Cases received and analyzed in I instance courts under 198(1) art. during 2007-2011

Year	Balance of unfinished cases in the beginning of reporting period	Cases received	Cases finished	Balance of unfinished cases in the end of reporting period	Duration of proceedings		
					Up to 6 months	From 6 up to 12 months	12 months and longer
2011	1	7	6	2	6	0	0
2010	0	5	4	1	4	0	0
2009	1	5	6	0	5	0	1
2008	0	0	0	0	0	0	0
2007	0	0	0	0	0	0	0

Source: Statistics of courts http://www.teismai.lt/lt/teismai/teismai-statistika

As one can see from table 3 stable and even increasing number of cases has been reaching courts since 2009, whereas, one can make a conclusion that this article is being really adjusted in practice and is such case it can be deriven to articles, under which criminal liability for cybercrimes is being adjusted.

It should be noted that under RF CC computer information should be understood as an information (messages, data) provided using support of electronic signals independent on storage, conversion or transmission ways of these, so we have a opinion that this concept does not include the concept "information systems".

Lithuanian criminal liability for unlawful influence on an information system can occur under RL CC 197 art. "Unlawful influence on an information system".

In RL CC 197 art. 1 p. criminal liability for unlawful disturbance or termination of the operation of an information system thereby incurring major damage is foreseen, and in 2 p. of this article criminal liability for the same acts in respect of an information system of strategic importance for national security or of major importance for state government, the economy or the financial system is foreseen.

Object of criminal act – orderly operation and management of information systems.

Thing of criminal act foreseen in 1 p. Of this article – any information system, and in 2 p. –just information systems of strategic importance for national security or of major importance for state government, the economy or the financial system. Legislator has not provided concept of an information system.

Information system – totality of technical and programming devices used for creation, sending, acceptance or other maintenance of an information in electronic way. This is very wide concept practically including the same computer, as well as computer systems or computer networks. <...> Legislator of CC has chosen the widest possible description of an information system, i. e. Natural technologically, regardless of information technologies or variety of these existing in concrete period of time[30].

Objective side of criminal act foreseen in RL CC 197 art. can occur in these alternative acts:

– unlawful (i.e. person has not been empowered by legal owner or possessor of an information system to make mentioned acts) disturbance of the operation of an operation system;

– unlawful termination of the operation of an information system.

In each of these cases it necessary for consequences to occur – disturbance or termination of the operation of an information system thereby incurring major damage. Furthermore, analogically as in RL CC 196 art. criminal act can be expressed with active acts (-s) acting and this (these) must be unlawful. Causality between made forbidden acts and incurred major damage is also necessary. Problem of understanding of major damage has already been discussed analyzing RL CC 196 art., so we will not repeat more.

Guiltiness form of this criminal act can be remarked both direct intent and indirect intent.

Subject of such criminal act – person of diminished capacity, whose age has been sixteen before making the crime. Moreover, juridical person is also liable for these crimes as under RL CC 20 art. has set conditions of criminal liability of juridical persons.

Following alternative punishments for unlawful influence on an information system – a fine or by arrest or by imprisonment for a term of up to four years; for unlawful influence on an information system of strategic importance for national security or of major importance for state government, the economy or the financial system – a fine or by arrest or by imprisonment for a term of up to six years

Attention should be paid on the fact that in 197 art. 2 p., as well as in RL CC 198(1) art. 2 p. Dangerousness of foreseen crime is being increased by the special thing of a crime – an informa-

30 *Comment of criminal code of the Republic of Lithuania. Special part. II volume*, Registrų centras, Vilnius, 2009, p.426.

Table 4. Cases received and analyzed in I instance courts under 197 art. during 2007-2011

Year	Balance of unfinished cases in the beginning of reporting period	Cases received	Cases finished	Balance of unfinished cases in the end of reporting period	Duration of proceedings		
					Up to 6 months	From 6 up to 12 months	12 months and longer
2011	0	3	2	1	2	0	0
2010	0	1	1	0	1	0	0
2009	0	0	0	0	0	0	0
2008	0	0	0	0	0	0	0
2007	0	0	0	0	0	0	0

Source: Statistics of courts http://www.teismai.lt/lt/teismai/teismai-statistika

tion system of strategic importance for national security or of major importance for state government, the economy or the financial system. We have in opinion that having executed criminal act foreseen in 197 art. 2 p., as well as in RL CC 198(1) art. 2 p. damage on such essential state interests as public security, state government, financial economic state interests and other, it should not be tolerated. Reaching to ensure maximum effectiveness, proportionality and detention for execution of mentioned criminal act of applicable sanctions the punishment should be strict. Under our opinion sanction – fine foreseen both in 197 art. 2 p., and in RL CC 198(1) art. 2 p. for the moment is too soft and inadequate to the crime under execution, so we would offer to deny a possibility to intend a fine both in 197 art. 2 p., and in RL CC 198(1) art. 2 p..

For the reason that analogically as in case of RL CC 196 art. discussed before as in case of analyzed RL CC 197 art. legislator has not provided clarification of concepts used; he has also foreseen that alternative punishments can be applied for the criminal act made, so practice of courts has a significant influence on how this article is being executed in real life. Below we provide a table about cases received and analyzed in I instance court in accordance with RL CC 197 art. during 2007-2011.

Evidentially, situation with entry of cases under RL CC 197 art. into the court is very bas – during three years no case of such type has been analyzed in the court of I instance, and during last two years four cases have been analyzed in these courts totally. Assumption on why could it be so have already been discussed in chapter 3.1. of this work, so

we will not repeat. Undoubtedly, conclusion that practice of courts in analysis cases under RL CC 197 art. is just under formation can be done, and evidentially, rather long period of time should pass for formation of common practice that could be ground for pretrial officers in analysis of similar type cases.

As we have already mentioned analyzing criminalization of unlawful access to information systems, under RF CC computer information should be understood as an information (messages, data) provided using support of electronic signals independent on storage, conversion or transmission ways of these, so we have a opinion that this concept does not include the concept "information systems". Whereas, we can state that criminal liability for unlawful influence on an operation system is not foreseen in RL CC as well (naturally, operation of an information system can be disturbed by breaking regulations of usage of computer systems in some cases, but this is not a necessary condition).

Under our opinion orderly operation of information systems is actually important wishing to ensure successful execution of functions of any entity or company, also granting that interests both of these systems and their users will not be violated. Egz., having disturbed or terminated operation of an information system any bank of data can provide signs appropriately stored in it rather distorted possibly resulting in break of reputation of natural or juridical persons, their financial interests, even public security of the state (officers releases of the person having made serious crime for having accessed that bank of data it is not shown that such a person is not under search in public) and sim.. Whereas, influence on an information system made by offender can disturb not only orderly performance of functions for that such information system is created, but also cause further negative consequences for their owners and users.

Furthermore, as a consequence of criminal connection to information systems acknowledgment with content of information is reached as possibly letting disruption of successful business or other crimes are being done during such connection more often, egz., non-public electronic data is being appropriated.

Therefore, summarizing the stated one can affirm that connection to information systems and influence on them is named as acts dangerous for society causing negative consequences, so under our opinion RL CC 28 chapter should be amended with articles criminalizing mentioned acts. Moreover, such

an opinion is grounded by legal norms of international documents recommending to criminalize both unlawful connection to an information system and unlawful influence on an information system, like previously in the work provided statistic of courts in accordance with cases under analysis in I instance courts (198(1) art. is possible to derive to one of the most often articles, under which criminal liability for cybercrimes is being applied).

Criminal liability for an inappropriate usage of installations

Criminal liability for an inappropriate usage of installations in Lithuania is foreseen in RL CC 198(2) art. "Unlawful disposal of installations, software, passwords, login codes and other data".

In RL CC 198(2) art. criminal liability for Unlawful disposal of installations, software, passwords, login codes and other data directly intended for the commission of criminal acts, producing, carriage or selling or other distribution or acquisition of these or storage having purpose to make criminal acts.

Object of criminal act foreseen in this article is security of electronic data and information systems, invasion of privacy of a person, property rights and property interests of persons, system of finances and sim..

Thing of criminal act – installations or software, also passwords, logins and other similar data directly intended for the commission of criminal acts. *Installations are an installed complex mechanism. These installations can be equipment or devices for various encryption, decryption, copying, scanning of information, connection to computer or computer network or making of other acts. Software – various computer viruses ("Trojans", logical "bombs", "wormseeds" and other.), programs for observation of networks and similar acts. Passwords, logins and other similar data – all data empowering to make acts an appropriate information system detects as own and authentifies the person as legal user of the system.*"[31]

Objective side of criminal act can be expressed with these alternative acts: producing, carriage or selling or other distribution or acquisition of installations, software, passwords, login codes and other data directly intended for the commission of criminal acts having the same purpose. Criminal liability is being

31 *Comment of criminal code of the Republic of Lithuania. Special part. II volume*, Registrų centras, Vilnius, 2009, p.438.

applied neither having made nor one of these acts.

From disposition of RL CC 198(2) article one can see the act of such type is being named as criminal in case two essential conditions are being executed during realization of it:

1.there must be a disposal of such installations, software, passwords, login codes and other data directly intended for the commission of criminal acts;

2.the disposal must be unlawful.

Notable, that producing or other disposal of installations or software, also passwords, logins and other data deriven for an authorized usage of data or an authorized check of information systems and their security is not being punished.

Attention should be paid on the fact that under this article it is not necessary to make real criminal act using support of such production, or some socially or materially negative consequences would occur after such criminal acts. For intention of criminal liability it is enough the fact of unlawful disposal of installations, software, passwords, login codes and other data directly intended for the commission of criminal acts.

Behold, Vilnius town district court has recognized J.P. as guilty under RL CC 1982 art. 1 p. and intended him a fine of 10 MSL (1,300 Lt) for he using personal computer had created false site of Internet banking service "X.net"of SC Bank internet, intended to fix codes and passwords of connection to an electronic banking service office station of the bank clients and also later to transfer these via Internet into created electronic mail boxes, and also has manufactured software intended to make crimes, exactly, to make criminal acts under RL CC 1981 art., 214 art., 215 art. and 182 art. Later he has resend mentioned false JC bankas "X" Internet site via Internet to M.J. and in such way he has unlawfully transmitted software intended to make crimes.[32] Whereas, J.P. had not been performing criminal acts personally by using his unlawfully manufactures software, but just for manufacturing such software and transmittance of it to other person his act is being qualifies under RL CC 1982 art.

Subjective side of such criminal act it is required to be remarked that form of guiltiness can be direct intention.

Subject of this criminal case – person, whose age has been sixteen before making the crime. Such person also must be of diminished capacity. Moreover, juridical person is also liable for these crimes as under RL CC 20 art. has

32 Vilnius town 1st district court, decision dated 14th of September 2009 in criminal case No. N1-1470-88/2009.

5 Table. Cases received and analyzed in I instance courts under 198(2) art. during 2007-2011

Year	Balance of unfinished cases in the beginning of reporting period	Cases received	Cases finished	Balance of unfinished cases in the end of reporting period	Duration of proceedings		
					Up to 6 months	From 6 up to 12 months	12 months and longer
2011	1	0	1	0	0	0	1
2010	1	2	2	1	2	0	0
2009	0	8	7	1	7	0	0
2008	0	0	0	0	0	0	0
2007	0	0	0	0	0	0	0

Source: Statistics of courts http://www.teismai.lt/lt/teismai/teismai-statistika

set conditions of criminal liability of juridical persons.

Criminal acts, for which liability is foreseen under 1981 art. and 1982 art. are deriven to group of mild crimes under leadership of CC 11 art. 3 part..

Unlawful disposal of installations, software, passwords, login codes and other data can be punished with one of these alternative punishments – community service or by a fine or by arrest or by imprisonment for a term of up to three years.

Having looked at 5 table one can make a conclusion that cases under this article has begun to enter Lithuanian cases just in 2009, when 8 cases have been received. However, no case under this article has been received in I instance courts in 2011 again.

Under our opinion in view of name RF CC 273 article "Creation, Use, and Dissemination of Harmful Computer Programs" is mostly similar to RL CC 198(2), so we will analyze are these articles really similar and is criminal liability for an inappropriate usage of installations foreseen in both of them more detailed.

In RF CC 273 art. 1 p. criminal liability for creation, dissemination or use of computer programs or other computer information, which are knowingly intended for unsanctioned destruction, blocking, modification or copying of computer information or for balancing-out of computer information security facilities is foreseen, in RF CC 273 art. 2 p. criminal liability for the same acts made by group of persons agreed in advance or organized group or person using advantage of its official position is foreseen, and in 3 p. of this article criminal liability for the same acts set in parts 1 and 2

of this article if they have entailed heavy consequences or have posed a threat of their occurred is foreseen.

Object of this criminal act – security, immunity of computer information and sim. so under our opinion object of RF CC 273 art. is narrower in comparison to RL CC 198(2) art., for it is focused on criminal acts against security of computer information, while object of RL CC 198(2) art. includes security not only of computer data, but also of information systems and immunity of privacy of a person, property rights of persons, system of finance and sim..

Common thing of RF CC 273 art. – harmful computer programs and other computer information, which are knowingly intended for unsanctioned destruction, blocking, modification or copying of computer information or for balancing-out of computer information security facilities.

Opinions of scientists stand out in special literature about that is "harmful computer programs". Considerable part of authors stand out that synonymous concepts "harmful programs "and "computer viruses".

S. V. Polubinskaya and S. V. Borodulin had shown that RF CC 273 art. "..speech is about creation of so called computer viruses by creating an appropriate computer programs, and also making modifications in already existing computer programs". Under our opinion one can not agree with such a view, for much more various harmful programs exist in nowadays world not only as "viruses", so comparing concepts "harmful programs" and "viruses" thing of criminal act foreseen in RF CC 273 art. is being rather narrowed.

A. G. Volevodz mentions that concept "harmful programs "is understood as programs created especially for restriction of normal operation of computer programs (without which further operation of electronic calculating machines, systems and networks is impossible).[33]

Y.I. Liagunov and A.V. Pushkin mention that harmful program is understood as specially written (created) program using that it is possible to make unauthorized acts and to make damage for the owner or possessor of information or other persons by blocking, modifying or copying information as a consequence[34].

33 Volevodz, A.G. (2002), *Actions against computer crimes: legal essentials of international cooperation* [*Protivodeistvie komp'yuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva*], Yurlitinform, Moscow, p. 73.

34 Vetrov, N.I., Lyapunov, Yu.I. (1998), *Criminal law. Special part*

We would agree with the position of these authors actually.

The mostly widespread harmful programs are being stated: computer viruses, "Trojans", "logical bombs "and other[35].

It stays unclear, what the legislator wished to say with a concept "other computer information" – could this concept include passwords, logins and sim., as in case of Lithuania? This question stays open for a while, for the new wording of RF CC 273 article is valid just for few months and there is no both practice of courts and comments of scientists that could let to provide clarification of this concept.

Objective side of criminal act can be expressed with these alternative acts:

– creation of computer programs or other computer information, which are knowingly intended for unsanctioned destruction, blocking, modification or copying of computer information or for balancing-out of computer information security facilities;

– dissemination of computer programs or other computer information, which are knowingly intended for unsanctioned destruction, blocking, modification or copying of computer information or for balancing-out of computer information security facilities;

– use of computer programs or other computer information, which are knowingly intended for unsanctioned destruction, blocking, modification or copying of computer information or for balancing-out of computer information security facilities.

Two first acts with that objective side can be expressed are rather similar to acts with that objective side of RL CC2) art. can be expressed. The third act with that objective side of RF CC 273 art. can be expressed is extremely different from objective side of RL CC 198(2) art. – liability is being foreseen for use of computer programs or other computer information, which are knowingly intended for unsanctioned destruction, blocking, modification or copying of computer information or for balancing-out of computer information security facilities. Egz. Frequently often use of computer receives letter polluted with viruses that are being forwarded to other without having any evil intentions or knowledge about this and in such way is already using a harm-

[*Ugolovnoe pravo. Osobennaya chast'*], Yurisprudentsiya, Moscow, p. 554.

35 Volevodz, A.G. (2002), *Actions against computer crimes: legal essentials of international cooperation* [*Protivodeistvie komp'yuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva*], Yurlitinform, Moscow, p. 73.

ful program. Can such a person extend a criminal liability? Reading disposition of RF CC 273 art. word to word, the answer should be – yes. In such case one is to doubt is the disposition of this article construed in an appropriate way for using such logic, practically each user of a computer can extend criminal liability. Under our opinion disposition of RL CC 198(2) art. is construed better in this case, under which criminal liability occurs for purposeful unlawful: producing, carriage or selling or other distribution or acquisition of harmful programs only.

From disposition of RF CC 273 art. one can see that act of such type is being named as criminal in case to essential conditions are being executed realizing it (practically, the same as foreseen in disposition of RL CC 198(2) art. as well):

1. computer programs or other computer information, which is knowingly intended to make criminal act, must be used;

2. possession must be unlawful, i.e. unsanctioned destruction, blocking, modification or copying of computer information or for balancing-out of computer information security facilities must be executed.

Notable, that under this article as under RL CC 198(2) art., it not demanded that real negative consequences occur, it is enough of the fact of creation or possession of harmful computer programs or other computer information.

Subjective side of RF CC 273 art. – direct intent only as in case of RL CC 198(2) art..

Aggravating circumstances, for which the crime is being named more serious are foreseen in RF CC 273 art. 2 and 3 part, as consequence of what more strict sanctions are foreseen this is concerned by legislator with:

– Subject of the crime and consequences of the crime or subjective side of the crime (necessary conditions):

-criminal act is being made by group of persons agreed in advance;

-criminal act is being made by an organized group. Under RL CC 60 art. in case act is made by a group of accomplices reorganized group this is being named as aggravating circumstance when sentencing;

-criminal act is being made by a person using advantage of its professional position;

-criminal act has caused major damage;

-criminal act has been made for selfish intentions.

– Under consequences of the crime only:

– criminal act has caused serious consequences or caused conditions for occurring these.

While in RL CC 198(2) art. no aggravating circumstances are set. We would think that it would be purposeful to see additional qualifying attribute in RL CC 198(2) art (as it has been done in RF CC 273 art.) – in case criminal act is being made by a person using advantage of its professional position. More detailed ground why this should be done has been given in 3.1. subsection of this work as analyzing the question of criminal liability for unlawful access to electronic data and influence on this, so we will not repeat in this part.

Subject of criminal act foreseen in RF CC 273 art. – person of diminished capacity. Whereas, different from RL CC 198(2) art., it is not set in RF CC 272 art. those juridical persons can be prosecuted. In case criminal act is being made by representative of juridical person liability goes on this natural person directly.

Under leadership of RF CC 15 art. 2 p. Criminal acts for that criminal liability is foreseen under 273 art. 1 p., 2 p. and 3 p., are deriven to group of less serious crimes.

In sanction of RF CC 273 art. 1 p. These alternative punishments are set – restraint of liberty for a term of up to four years, or by compulsory labor for a term of up to four years, or by deprivation of liberty for the same term with a fine in the amount up to 200 thousand rubles, or in the amount of a wage/salary or any other income of the convicted person for a period up to eighteen months, in RF CC 273 art. 2 p. – restraint of liberty for a term of up to four years, or by compulsory labor for a term of up to five years with deprivation of the right to hold specified offices or to engage in specified activities for a term of up to three years or without such, or by deprivation of liberty for a term of up to five years with a fine in the amount of 100 thousand to 200 thousand rubles or in the amount of a wage/salary or other income of the convicted person for a period of two to three years or without such and with deprivation of the right to hold specified offices or to engage in specified activities for a term of up to three years or without such, in RF BK 273 art. 3 p. – deprivation of liberty for a term of up to seven years. Comparing with sanction foreseen in RL CC 198(2) art. one can make a conclusion that more strict punishments for this crime are foreseen in Russia (egz. maximum restrain of liberty punishment in Russia can be for a term of up to seven years, and in Lithuania – three years), furthermore, in RF CC 273

art. some "double punishments"(egz. restraint of liberty and fine) are foreseen differently than in an appropriate article of RL CC.

Criminal liability for violation of rules of operation and access

There is no criminal liability for making a criminal act accorded to violation of rules of operation and access foreseen in RL CC. While, criminal liability for violation of rules of operation and access can incur under RF CC 274 art. "Violating the rules for operation of the facilities for computer information storage, processing and transmittance and of information-telecommunication networks,"

In RF CC 274 art. 1 p. Criminal liability for violation of the rules for operation of the facilities for computer information storage, processing and transmittance or of information-telecommunication systems and of terminal equipment, as well as of the rules for access to information-telecommunication networks, that has entailed the destruction, blocking, modification or copying of computer information accompanied by causing a major damage is foreseen, in RF CC 274 art. 2 p. Criminal liability for the same activity, if it has entailed heavy consequences or a threat of their occurrence, is foreseen.

Object of RF CC 274 art. safe and orderly operation, storage or transmittance of secured computer information or information-telecommunication networks and terminal, as well as safe and orderly connection to information-telecommunication networks.

Thing of this criminal activity – secured rules for operation of the facilities for computer information storage, processing and transmittance and of information-telecommunication networks, as well as rules of connection to information-telecommunication networks.

Objective side of RF CC 274 art. is being expressed with acts violating rules for operation of the facilities for computer information storage, processing and transmittance and of information-telecommunication networks.

From disposition of RF CC 274 art. one can see that such activity is being named as criminal in case these essential conditions are being executed during its realization:

1. Negative consequences occur – computer information must be destroyed, blocked, modified or copied and major damage must be caused by this;

2. causality meaning that actually for the criminal act made by the offend-

ing has caused necessary negative consequences.

Subject of criminal act foreseen is RF CC 274 art. – natural person of diminished capacity.

Under leadership of RF CC 15 art. 2 p. Criminal acts liability under that is foreseen in 274 art. 1 p. and 274 art. 2 p., are being deriven to group of less serious crimes.

In sanction of RF CC 274 art. 1 p. These alternative punishments are set – a fine in the amount of up to 500 thousand rubles or in the amount of a wage/salary or other income of the convicted person for a period of up to eighteen months, or by corrective labor for a term of six months to one year, or by restraint of liberty for a term of up to two years, or by compulsory labor for a term of up to two years, or by deprivation of liberty for the same term, in RF CC 274 art. 2 p. – compulsory labor for a term of up to five years, or by deprivation of liberty for the same term.

Under our opinion RF CC 274 art. essentially differs from articles fixed in RL CC XXX chapter. This is blanket norm deriving into detailed rules, while, in the chapter of RL CC as analyzed no such articles exist. Accordingly, on the other side we think that, essentially, unlawful connection to an information system or unlawful influence on this system is being done, when violating the rules for operation of the facilities for computer information storage, processing and transmittance or of information-telecommunication systems and of terminal equipment, as well as of the rules for access to information-telecommunication networks.

Generalizing the stipulated one can make a conclusion that majority of cybercrimes liability for these is foreseen in criminal codes of the state are being deriven to group of less serious crimes and just few of these – to group of mild crimes both in Lithuania and in Russia.

Having made analysis of norms of criminal codes of Lithuania and Russia regulating composition of separate cybercrimes the conclusion can be made that both in RL CC and in RF CC criminal liability for unlawful access to electronic data, possession of harmful programs is foreseen, but in RF CC direct criminal liability for connection to an information system or for an unlawful influence on an information system, as well as direct criminal liability for breaches of rules of use of computer system in RL CC is not foreseen.

Having in opinion that natural person of diminished capacity, whose age has been sixteen before making the

crime can be subject of cybercrimes of both compared states, but in Lithuania different than in Russia juridical person can also be prosecuted. Sanctions for cybercrimes do not differ essentially by their size, but for the most serious criminal acts deprivation of liberty can be made as a punishment in Russia only. We have a opinion that having analyzed that having made criminal act set in 196 art. 2 p., as well as in 197 art. 2 p., and also in RL CC1) art 2 p. the damage is being made for such essential state interests as public security, state government,, state economic, financial interests and other, it should not be tolerated and reaching to grant the maximum effectiveness, proportionality and deterrent of completion of mentioned criminal act, the punishment should be strict. Under our opinion in 196 art. 2 p., 197 art. 2 p. and in RL CC 198(1) art. 2 p. alternative punishment – a fine as set for the moment is rather soft and inadequate for criminal act is being made, so we would offer to deny possibility of attending a fine in sanctions of mentioned articles.

In RF CC differently than in RL CC more alternative punishments and possibility of "double punishment" is foreseen (egz. a fine together with deprivation of liberty). Under our opinion such huge variety of alternative punishments should not be foreseen in sanction for this widens possibilities of corruption in pretrial and trial investigation and composes conditions for attending markedly different punishments for essentially identical cybercrime.

Notable that differently to RL CC in RF CC clarification of concepts "computer information" and "major damage" is provided in such way solving a problem of unequal stating of these concepts together with a problem of qualification of the act. Under our opinion it would be well to amend RL CC XXX chapter with one more article providing clarification of very abstract concept "major damage" by revealing both pecuniary and none pecuniary aspects of this concept. In such way a problem of unequal stating of these concepts together with a problem of qualification of the act would be avoided. Moreover, such practice to provide clarification of concept is being applied in the same RL CC, egz. RL CC 190 art. value of property is clarified as applied for crimes of XXVIII chapter.

Having analyzed statistic of cases under articles 196-198 2p. received and analyzed in I instance courts, we see that really essential and mostly often articles cases under these reach the court during 2007-2011 are 198 and 1981 art. Unfortunately, paying attention on the fact that

modifications of RF CC 28 chapter have been made just few months ago, we are not able to provide statistic, of the last five years i.e. 2007 – 2011, how many cases under appropriate articles have been received and analyzed in I instance courts of Russia.

Conclusion

1. Major part of cybercrimes for these criminal liability is foreseen in criminal code of an appropriate state is being deriven to group of less serious crime both in Lithuania and Russia, and just few of these crimes are being deriven to group of mild crimes.

2. Having analyzed separate attributes of composition of cybercrimes of the Republic of Lithuania and Russian Federation the statement was that essentially both in RL CC and RF CC criminal liability for unlawful access to electronic data and influence on it, possession of harmful programs is foreseen, but direct criminal liability for unlawful connection to an information system or unlawful influence on an information system is not foreseen in RF CC, and in RL CC – for violation of the rules of use of computer system.

3. In both comparative states natural person of diminished capacity, whose age has been sixteen before making the crime can be subject of cybercrimes of both compared states, but in Lithuania different than in Russia juridical person can also be prosecuted. Paying attention on the fact that more and more cybercrimes are being made by employees using the advantage of their professional position, also on fact that persons that have access to important electronic data for their duties taken can cause more major damage more often than other persons, we would think that more strict liability should be set to the special subject – person making criminal act using advantage of its professional position in articles of RL CC XXX chapters as it has been done in two articles of RF CC 28 chapter.

4. Having made comparative analysis of sanctions of cybercrimes set in RL CC and RF CC it has been set that sanctions for cybercrimes do not differ mark able in both states, but for the most serious criminal acts deprivation of liberty can be made as a punishment in analyzed articles of RF CC only. We have a opinion that having analyzed that having made criminal act set in 196 art. 2 p., as well as in 197 art. 2 p., and also in RL CC[1)] art 2 p. the damage is being made for such essential state interests as public security, state government,, state economic, financial interests and other,

it should not be tolerated and reaching to grant the maximum effectiveness, proportionality and deterrent of completion of mentioned criminal act, the punishment should be strict. Under our opinion in 196 art. 2 p., 197 art. 2 p. and in RL CC 198(1) art. 2 p. alternative punishment – a fine as set for the moment is rather soft and inadequate for criminal act is being made, so we would offer to deny possibility of attending a fine in sanctions of mentioned articles.

In RF CC differently than in RL CC more alternative punishments and possibility of "double punishment" is foreseen (egz. A fine together with deprivation of liberty). Under our opinion such huge variety of alternative punishments should not be foreseen in sanction for this widens possibilities of corruption in pretrial and trial investigation and composes conditions for attending markedly different punishments for essentially identical cybercrime.

5. Differently to RL CC in RF CC clarification of concepts "computer information" and "major damage" is provided in such way solving a problem of unequal stating of these concepts togehter with a problem of qualification of the act. Under our opinion it would be well to amend RL CC XXX chapter with one more article providing clarification of very abstract concept "major damage" by revealing both pecuniary and none pecuniary aspects of this concept. In such way a problem of unequal stating of these concepts together with a problem of qualification of the act would be avoided.

6. Having analyzed statistic of cases under articles 196-198 2p. received and analyzed in I instance courts, we see that really essential and mostly often articles cases under these reach the court during 2007-2011 are 198 and 198[1] art. Unfortunately, paying attention on the fact that modifications of RF CC 28 chapter have been made just few months ago, we are not able to provide statistic, of the last five years i.e. 2007 – 2011, how many cases under appropriate articles of RF CC have been received and analyzed in I instance courts of Russia.

References

1. "Actual cassation decisions in criminal cases during period 11th – 20th of February 2012" ["Aktual'nye kassatsionnye opredeleniya po ugolovnym delam za period s

11 po 20 fevralya 2012 goda"], available at: http://oblsud.ynao.sudrf.ru/modules.php?name=press_dep&op=1&did=538

2. *Comment of criminal code of the Republic of Lithuania. Special part. II volume*, Registrų centras, Vilnius, 2009, 695 p.
3. "Criminal code of the Republic of Lithuania", *Official Gazette*, 2000, No. 89-2741.
4. "Criminal code of the Republic of Lithuania", *Official Gazette*, 2004, No. 25-760.
5. "Criminal code of the Republic of Lithuania", *Official Gazette*, 2007, No. 81-3309.
6. "Federal law of the Russian Federation on 7 December 2011 No. 420-FZ "On amending the Criminal code of the Russian Federation and separate legislative acts of the Russian Federation" ["Federal'nyi zakon Rossiiskoi Federatsii ot 7 dekabrya 2011 g. N 420-FZ "O vnesenii izmenenii v Ugolovnyi kodeks Rossiiskoi Federatsii i otdel'nye zakonodatel'nye akty Rossiiskoi Federatsii"], available at: www.rg.ru/2011/12/08/p-raboty-site-dok.html
7. Gavrilin, Yu.V. (2003), *Crimes in the sphere of computer information. Qualification and evidence: study guide* [*Prestupleniya v sfere komp'yuternoi informatsii: kvalifikatsiya i dokazyvanie: Ucheb. posobie*], YuI MVD RF, Moscow, 245 p.
8. Gul'bin, Yu., "Crimes in the sphere of computer information" ["Prestupleniya v sfere komp'yuternoi informatsii"], available at: www.lawmix.ru/comm/8288/
9. Karelina, M.M., "Crimes in the sphere of computer information" ["Prestupleniya v sfere komp'yuternoi informatsii"], available at: www.crime-research.ru/library/CodeRu.htm
10. Kozachenko, I.Ya., Neznamov, Z.A. (1998), *Criminal law. Common part* [*Ugolovnoe pravo. Obshchaya chast'*], Norma, Infra-M, Moscow, 516 p.
11. "Law of the Republic of Lithuania on electronic signature", *Official Gazette*, 2000, No. 61-1827, Art. 2, 8.
12. Mazurov, V.A. (2002), *Computer crime: classification and methods of countering* [*Komp'yuternye prestupleniya: klassifikatsiya i sposoby protivodeistviya*], Logos, Moscow, 148 p.
13. Naumov, V., "National legislation in the fight against computer crime" ["Otechestvennoe zakonodatel'stvo v bor'be s komp'yuternymi prestupleniyami"], available at: www.hackzone.ru/articles/a5.html

14. Piesliakas, V. (2006), *Lithuanian criminal law. The first book*, Justitia, Vilnius, 300 p.
15. Stitilis, D. (2011), *Cybercrimes. Methodic measure*, Mykolas Romeris university, Vilnius, 264 p.
16. "The Decision of Dzerzhinsky town court dated 27th of July 2011 Case No (not defined)" ["Delo No. (ne opredeleno) Prigovor imenem Rossiiskoi Federatsii, g. Dzerzhinsk 27 iyulya 2011 goda"], available at: www.gcourts.ru/case/1446171
17. Vetrov, N.I., Lyapunov, Yu.I. (1998), *Criminal law. Special part* [*Ugolovnoe pravo. Osobennaya chast'*], Yurisprudentsiya, Moscow, 635 p.
18. Volevodz, A.G. (2002), *Actions against computer crimes: legal essentials of international cooperation* [*Protivodeistvie komp'yuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva*], Yurlitinform, Moscow, 197 p.

Криминализация опасных деяний в киберпространстве в уголовных кодексах Литвы и России: сравнительный аспект

Штитилис Дарюс
Доктор юридических наук, профессор,
заведующий комитетом программы «Право новых технологий»,
Университет Миколаса Ромериса,
08303, Литва, Вильнюс, ул. Атейтес, 20;
e-mail: stitilis@mruni.eu

Клишаускас Валдас
Ассистент,
Университет Миколаса Ромериса,
08303, Литва, Вильнюс, ул. Атейтес, 20;
e-mail: stitilis@mruni.eu

Аннотация

В статье проанализированы правовые нормы Уголовных кодексов Литовской Республики и Российской Федерации относительно киберпреступлений в сравнительном аспекте, выявлены проблемы правового регулирования киберпреступлений, а также предложены возможности для решения таких задач.

Ключевые слова

Киберпреступность, правовое регулирование, криминализация опасных деяний в киберпространстве.

Библиография

1. Актуальные кассационные определения по уголовным делам за период с 11 по 20 февраля 2012 года. [Электронный ресурс]. – Режим доступа: http://oblsud.ynao.sudrf.ru/modules.php?name=press_dep&op=1&did=538.
2. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2002. – 197 с.
3. Гульбин Ю. Преступления в сфере компьютерной информации. [Электронный ресурс]. – Режим доступа: www.lawmix.ru/comm/8288/.
4. Дело № (не определено). Приговор именем Российской Федерации, г. Дзержинск 27 июля 2011 года. [Электронный ресурс]. – Режим доступа: www.gcourts.ru/case/1446171.
5. Карелина М.М. Преступления в сфере компьютерной информации. [Электронный ресурс]. – Режим доступа: www.crime-research.ru/library/CodeRu.htm.
6. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия. – М.: Логос, 2002. – 148 с.
7. Наумов В. Отечественное законодательство в борьбе с компьютерными преступлениями. [Электронный ресурс]. – Режим доступа: www.hackzone.ru/articles/a5.html.
8. Преступления в сфере компьютерной информации: квалификация и доказывание: Учеб. пособие / под ред. Ю.В. Гаврилина. – М.: ЮИ МВД РФ, 2003. – 245 с.

9. Уголовное право. Общая часть / под ред. Козаченко И.Я., Незнамова З.А. – М.: Норма, Инфра-М, 1998. – 516 с.
10. Уголовное право. Особенная часть / под ред. Н.И. Ветрова и Ю.И. Ляпунова. – М.: Юриспруденция, 1998. – 635 с.
11. Федеральный закон Российской Федерации от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». [Электронный ресурс]. – Режим доступа: www.rg.ru/2011/12/08/p-raboty-site-dok.html.
12. Comment of criminal code of the Republic of Lithuania. Special part. II volume. – Vilnius: Registrų centras, 2009. – 695 p.
13. Criminal code of the Republic of Lithuania // Official Gazette. – 2000. – № 89-2741.
14. Criminal code of the Republic of Lithuania // Official Gazette. – 2004. – № 25-760.
15. Criminal code of the Republic of Lithuania // Official Gazette. – 2007. – № 81-3309.
16. Law of the Republic of Lithuania on electronic signature // Official Gazette. – 2000. – № 61-1827. – Art. 2, 8.
17. Piesliakas V. Lithuanian criminal law. The first book. – Vilnius: Justitia, 2006. – 300 p.
18. Stitilis D. Cybercrimes. Methodic measure. – Vilnius: Mykolas Romeris university, 2011. – 264 p.