trial Detention", "On Ensuring the Safety of Persons Participating in Criminal Procedure" and departmental by-laws - legal acts.

The article presents the opinions of domestic scientists of penitentiary orientation regarding the content of the concept of security convicted persons in the custodial settings in the science of criminal enforcement law and the current legislation.

The article identifies six forms of ensuring the right of convicts to personal security: determination by the administration of the criminal correctional facilities the criterion of personal security of convicts; legal regulation of the personal security of prisoners; the authorities using risk-management measures; further resolving the issue of the place of serving the convicted person; ensuring the safety of convicts in connection with their involvement in criminal proceedings.

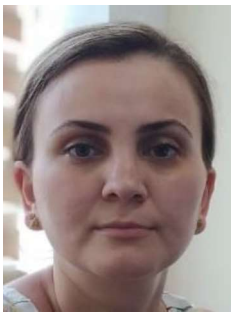
The author conducted a historical analysis of the formation and development of security issues of convicts in the normative acts of the Ukrainian Soviet Socialist Republic and independent Ukraine.

The author argues that there are many reasons for the threats to the personal safety of prisoners in criminal correctional facilities.

The article defines the concept of security convicted persons in the custodial settings - it is regulated by the current legislation and is provided by the staff of the bodies and criminal correctional facilities the protection of the rights and freedoms and legitimate interests of the prisoners while serving their sentences.

Keywords: *problem, security of prisoners, criminal correctional facilities, penitentiary institution, Ministry of Justice of Ukraine.*

УДК 343.3/.7
DOI: 10.31733/2078-3566-2020-2-151-157



Aytakin IBRAHIMOVA©
PhD in Law
(the Baku State University, Azerbaijan)

CYBERCRIMES AND STRUGGLE AGAINST THEM

Айтакін Назім Ібрагімова. Кіберзлочини та протидія їм. Зміни в традиційному настрої в цифровому суспільстві також вплинули на правопорушення. Кіберзагрози, які стали нагальними, мають широке коло змісту і не можуть регулюватися конкретним галузевим законодавством. Ще одна проблема полягає в тому, що об'єкт і суб'єктивна структура кіберзагроз дуже складні. Вони спрямовані не тільки проти конкретного громадянина, але навіть негативно позначаються на моральності великої нації (наприклад, інформаційні війни). Всі ці факти вимагають розробки пропозицій і рекомендацій щодо запобігання кіберзагрозам.

У сучасному світі, ІКТ слід розглядати як найпростіший спосіб вчинити злочини, спираючись на те, що ІКТ охоплюють всі людські життя і їх використання в кримінальних цілях є поширеним явищем. У цьому випадку, нелогічно припустити, що всі злочини в кіберпросторі є кіберзлочинності. Тому що об'єкт і мотив злочинних дій різні. З іншого боку, багато порушень, скоєних у кіберпросторі може здійснюватися традиційними способами. Посилаючись на це, стаття порушень в кіберпросторі ділиться на дві групи: традиційні порушення і порушення, які зазіхають на комп'ютерну інформацію. У першій групі ІКТ діє як засіб незаконної дії, а друга група не може здійснюватися без ІКТ.

Технологічні досягнення, використання систем штучного інтелекту та Інтернет речей потребують частих оновлень щодо класифікації кіберзлочинності. Тому важливо, щоб криміналізації і боротьби з новими порушеннями в кіберпросторі шляхом додавання нових підкатегорій до традиційної класифікації.

Ключові слова*: інформаційна безпеки, кіберправопорушення, кіберзлочини, класифікація кіберзлочинів, кібервійна, бази даних, доступність, конфіденційність, повнота*

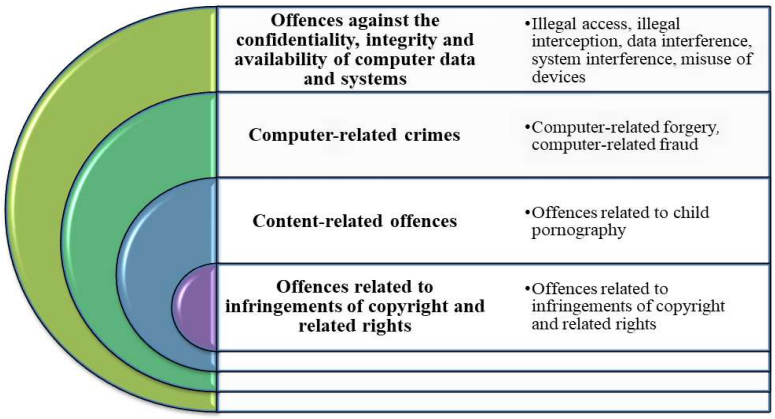
Problem statement. *"Cybercrime",* a concept formed as a result of rapid development of ICT, has a wide range of content. The term "computer crime" is also used in literature. In our opinion, the second concept is the result of a technical approach and the first concept should be consid-

© Ibrahimova A.N., 2020
ORCHID ID: https://orcid.org/0000-0002-3134-8486
aytakin_ibrahimli@yahoo.com

ered acceptable because of expanse. An interesting point is that cyberspace has a very wide range of resources, not just computer-related crimes are committed there, but also other illegal activities (fraud, copyright infringement, defamation, slander, etc.). are implemented, using cyberspace, i.e. existing relations and technical means can act as new ways to commit traditional crimes. So, do limits of "cybercrime" notion of increase? Is legitimate stand right regarding recognition of computer-related crimes in the criminal legislation to be justified as cybercrime? – Such questions prove the relevance of the research topic of the article.

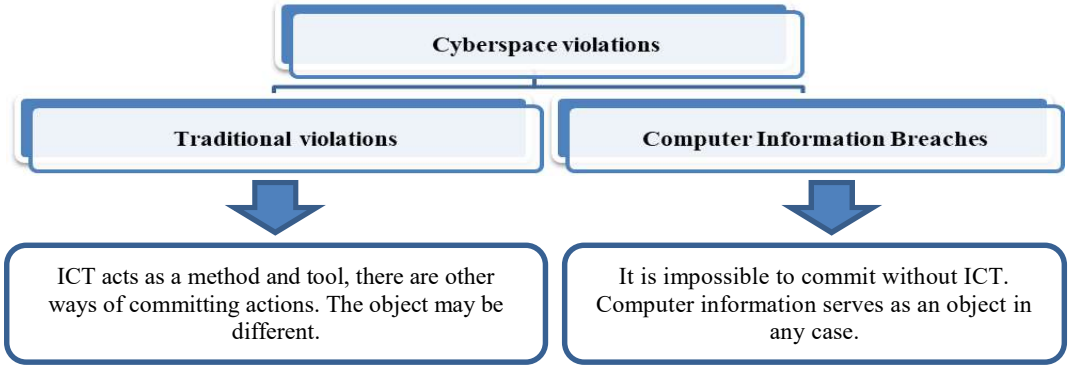
The article's objective is to determine the content of the term "cybercrime", analyze the international and national framework in this regard, determine the classify cybercrimes and make suggestions and recommendations on measures to struggle against cybercrimes.

Basic content. In the Budapest Convention (23 November 2001) cybercrimes are classified to the following types:



The Convention divides cybercrime into computer crimes and computer-generated crimes. In fact, we can agree with the position of the Convention. Because all of the above-mentioned crimes are committed in cyberspace. Criminal legislation of the Republic of Azerbaijan definitely sanctioned all of these acts. They are dealt with not just in the chapter of cybercrime, but also in different chapters. Today ICT should be regarded as the easiest way to commit crimes, based on the fact that ICT covers all human lives and their use for criminal purposes is widespread. In this case, it is not logical to consider all crimes, committed by the use of cyber environment, as cybercrime. Because the object and motive (purpose) of criminal acts are different. On the other hand, many actions can be conducted in cyberspace using traditional methods. For example, the circulation of child pornography as provided by Article. 171-1 of the Criminal Code of the Republic of Azerbaijan – spread, advertising, sale, transfer, sending, offering child pornography, create conditions for its acquisition; accompanied by preparation, acquisition or keeping for the purpose of spreading or advertising.Such pornographic products can be distributed not only in cyberspace, but also in the form of various publications, products and materials. The approach of the legislation of the Republic of Azerbaijan can be considered acceptable referring to them. Simply taking into account the specifics of an ICT-driven environment, it is advisable to make changes on the way of commitment of changes. Another issue is that terrorism and other such kind of dangerous crimes remained beyond the scope of the Convention. The spread of open calls for various types of terrorism (e.g, ISIS) on Twitter, Youtube and other networks demands an increased list of computer-based crimes.

The following conclusion can be made based on the aforementioned:



There are other official classifications along with one reflected in the aforementioned Convention. One of such classifications was made by the Interpol working group in 1991. All codes in this classification, have an identifier that starting with the letter "Q". They are also divided into 6 groups depending on the type of intent, where the letters "A", "F", "D", "R", "C", "Z" are used. For example, code consisting of the letter combination QA - unauthorized (unsanctioned) access and perception, QF code - computer fraud, QR code - illegal photocopying (piracy), etc. Each of these codes has its own classification, depending on the way of crime committment. Consistency in each classification goes towards reducing the public risk of crime [1, p. 415].

Interpol coding, embedded in the automated search information system, has wide potential to detect many cybercrimes.

QA – Unauthorized access and interception	•computer grappling (hacking), unauthorized access to computer information or network, interception of information and others
QD – Change of computer data	•a logic bomb, Trojan horse, «worm» computer virus and others
QF – Computer fraud	•fraud with ATMs, with slot machines, with means of payment, telephone fraud and others
QR – Illegal copying	•copying of computer games, software, topographies of semiconductor devices and others
QS – *Computer sabotage*	•malfunction of electronic data processing machine, destruction, blocking information and others
QZ – Other computer-related crime	•computer espionage, use of computer bulletin boards for criminal activities and others

The classification given by Debra Littlejohn Shinder is more widely assessed amidst unofficial classifications. Thus, D.L.Shinder distinguishes two categories of cybercrime: crimes committed by violent or potentially violent criminals and nonviolent crimes. The author includes cyberterrorism, assault by threat, cyberstalking, child pornography to violent or potentially violent cybercrimes.

D.L.Shinder divides nonviolent cybercrimes into various subcategories: cybertrespass, cybertheft, cyberfraud, destructive cybercrimes, other cybercrimes. D.L.Shinder classifies different crimes within each subcategory. For example, cybertheft has types like embezzlement, unlawful appropriation, corporate/industrial espionage, plagiarism, piracy, identity theft and DNS cache poisoning. The author's citation of other cybercrime as a separate subcategory will allow the classification of new criminal offenses that occur in cyberspace as the society progresses [2, p. 19-33].

There are different ways of committing cybercrime. According to 2016 data, the weakest point of information security is human factor and four most known types of attacks against it are

very common in Azerbaijan [7]:

1. Social engineering, Human hacking. Social engineering – collecting information from people by interaction with them. One of main factors of this type is deceive user by the use of fake profiles (by other name or any fake company, campaign, etc.) and virtual friendship and acquaintance. Basic purpose is to collect information by abuse of dating, virtual friendship or any other reliable source. Therefore, it is important for users to pay particular attention to the address of the letter. A fake site can be created even with a single letter change. (for example, www.facabook.com instead of www.facebook.com)

2. Brute-forcing. "Brute-force" is attack on a user's e-mail account or a password set on another account. In this case, passwords in the account are manually (one by one) or automatically verified by various means, using user information (e.g. name, surname, parent or child's name and date of birth, machine number, phone number, etc.) and password is found. So what is the purpose of brute-force attack? These attacks, such as social engineering, also aim to collect user data and subsequently use of that information for illegal purposes. According to the recommendations of the CERT, password security rules must be followed to protect against such attacks. For example, non-use of the same password on social networks, e-mails or other accounts. This case can lead to the "perception" of other accounts, if the password of one account is broken. At the same time, it would be good the user does not use his/her own data when setting passwords. For example, name, date, day or month of birth adjacently are usually used as password as a rule. Such types of passwords, easier to detect facilitates perpetrator's work. Therefore, it is considered rational to keep users away from such passwords. Moreover, the use of double authentication to prevent user's passwords from getting into the hands of malware is considered a modern and successful tool. Double biometric passwords were used for double authentication since 2015, while earlier the method of setting more passwords and sending SMS (message) to the mobile device was used.

It means, that not only fingerprints that turned to biological markers, but also iris are also used for identification. This method, widely used in mobile banking is already applied in last models of new phones. We believe that, biometric data is more "reliable" for identification and that further research and practice application in this area can play an indispensable role in ensuring information security. On the other hand, it is easier and more convenient to use biometric data rather than to remember different passwords.

3. Malware programmes. Malware technique is a way of downloading malicious software to the computer (Trojans, spyware, worms, viruses and botnets) by sending the user video, pictures, music, movies, any files or links. Main purpose of these programs is to steal information from the target.

It is worth noting that, malware that prevents users from using the Internet normally is continuing to grow and the measures to struggle against them are being strengthened. For example, the CERT makes recommendations like installation of firewalls to protect against botnets, regularly updating operating systems, browsers and other softwares from the producers' official website, not receiving files from unknown users and attachments (files) from unknown resources, being careful upon downloading files, etc. [8, p. 4].

4. Fishing. Fishing means "to fish" in English and is a kind of fraud reminiscent of global fishing. So, a swindler (fisher) is trying to trick the Internet users by the "trap" on the Internet. Fisher investigates bank accounts, credit cards and information needed to access to Internet of Internet users in different ways. Fishing is a special type of cyberbullying that forces users to submit personal information, usually of a financial nature, by way of fraud. A swindler creates fake website seeming as bank site (or any other financial-activity site, such as eBay). Criminals then try to trick users into this site to get confidential information such as login, password or PIN. Swindlers often distribute links to these sites with the help of spam. So how can we distinguish such fake websites from legitimate websites? –Determination of fishing threats and ways of protection from them are mentioned in the recommendations worked up by the Center of Electronic Security for users in this regard. For example, the presence of expressions in the form "Our dear customers" in the letter sent to the user indicates that the sender does not recognize the user. Writing one letter wrongly upon typing a webpage can even cause a user to fall into a "trap". The drop-down page can be very similar to the website he/she wants to access. Therefore, if the user is not careful and cautious, data may have be stolen long before a certain stage (for example, when you enter www.micrsoft.com, instead of www.microsoft.com, a very similar page might appear).

The ways of committing cybercrimes increase as ICT develops and adequate measures of

struggle should be strengthened. Because this type of crimes is characterized by a high latency level, which is caused by the specifics of their committing methods. Almost most researchers distinguish between four types of cybercrime depending on latency level [11, p. 171-176: 12]:

The first group includes crimes which no law enforcement agencies or victims have any information about the incident. It is called "natural latency". "Problem of disclosure" dominates in this type of crimes.

The second group includes crimes related to non-informing law enforcement by those responsible for reporting cybercrime. It is regarded as "artificial latency" and there arises "non-informing problem".

The third group includes the latent crimes as a result of improper assesment of the action and non-display of evidence of a criminal act because of low professionalism of the investigators despite law enforcement agencies are reported about cybercrime. It is called "borderline or partial latency" in literature.

The fourth group includes cybercrimes, which law enforcement agencies are informed about and that not registered due to various assumptions (hiden or concealed crimes).

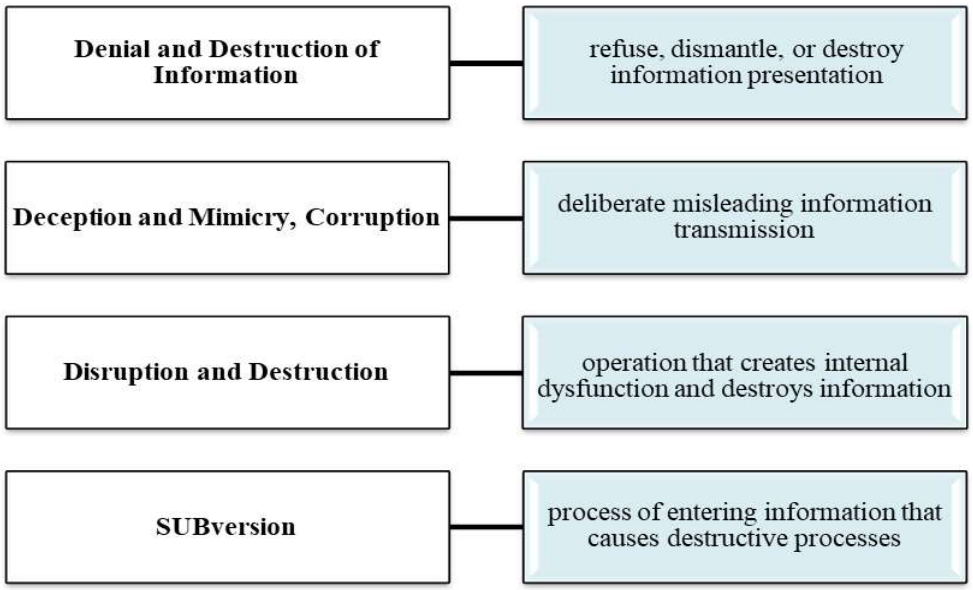
Information wars as a type of cybercrimes

Information conflict – information operations aimed at the destruction or control of the information resources of the other party, using specific methods, methods and means of affecting information resources. ***Information attacks*** are operations directed to the transfer, modification and destruction of information in any form without permission, as well as software, technical devices where confidential information is stored and human psychology. ***Information war*** is a more dangerous form of information effect, combining operations such as information attacks and information conflicts. It is a purposeful activity aimed at gaining advantage of information by damaging the information, information processes and systems of the other party; capturing economic and military potential of counterpart; changing people's behavior by influencing public consciousness. Information acts as an object of a weapon, target and defense in the information war. The sources refer information war to combined cybercrime [9, p. 57].

The terms "network war" and "cyber war" are suggested in the literature due to some stands of the authors. They consider network war to be more of a conceptual conflict of society of public level, arguing that it embraces economic, political and social spheres, while, cyber war has military purposes [5, p. 27-30].

There are also ideas about conducting information war in two directions: information-technical war and information-psychological war. Attack operations to different types of information systems (databases, analytical systems, etc.), telecommunication tools, computer networks and other technical tools are implied in information and technical warfare. Consequently, the operations of percepting, controlling, or destroying information systems are being implemented. The target is individuals, social groups, organizations, citizens of one or more states, and the world community in the information and psychological war. In fact, such a division is a logical contradiction. On the one hand, given the fact that the goals and strategies of the information war (political, military, economic, etc.) are important aspect, the technical characterization of such a dangerous operation system does not reveal its true essence. Because the purpose of the activity in each case, is a key factor. On the other hand, today psychological warfare is impossible without the use of such information systems, and technical operations are also carried out there. Therefore, it would be more appropriate to differentiate information warfare from objectives and strategy aspect. Technical operations including information perception, damage, alteration, destruction, etc. should be regarded as methods of realization of information warfare.

It is noted that basic paradigm of the information war consists of the following information operations:



Aforementioned division, which explains the information war in more technical terms, is not sufficient to respond the questions that arise from information and legal aspect. In our opinion, the classification of US researcher, Martin Libicki on the issue is more profound. The author distinguishes seven forms of information warfare [6, p. 7-8]:

- *Command and Control Warfare* is an information war aimed at linking commander and executor communication channels. Anti-head operations widespread in the past, and anti-neck operations widely developed presently and functioned with the use of ICT are applied in this type of warfare.
- *Information-based Warfare* is the process of collecting important information and at the same time protection of information resources by the attacking party.
- *Electronic Warfare* is a war against electronic communications. Electronic communication means include radio communication, radars and computer network. Main object of this type of war, which become more widespread since the formation of the electronic state is cryptographic trends. It is precisely the result of growing of such wars, that special rules are established in our republic for the protection of information resources of state importance.
- *Psychological Warfare* is a type of war that affects people's psychology. M.Libicki distinguishes four categories of psychological war: operations against national will, operations against leadership (command), operations against soldiers in the military, and other operations, war of cultures [6, p. 35].
- *Hacker Warfare* – diversion, targeted civilian objects of the opposite party. The weapons of the hackers are viruses.
- *Economic Info-Warfare*. M.Libicki describes this conflict in two ways: information blockade and information imperialism. The researcher evaluated the information blockade as a version of the economic blockade and reasoned that the disruption of the information would result in disruption of the economic sector - trade relations. The author interprets information imperialism as part of the general economic imperialism policy and views trade as a war. He argues that gaining privilege in trade results in privilege of knowledge in those countries and these countrie constantly try to "exert pressure" on "weaker states" not to miss a dominant position [6, p. 67-74].
- *Cyberwar.* The last classification, cyberwar become one of the most urgent problems of our time. In particular, information terrorism is characterized by its dangerous nature. As is known, the whole information is placed in information systems since all states move to e-state structure. It would be possible to "paralyze" the state not only in its political, military, but also economic, social and other areas by "attacking" its information industry. It should be noted that, the acceleration of gradual virtualization around the world keeps people away from real beings, which stipulates the formation of simulated wars. Military operations in real polygon are replaced by computer model in these wars.We can confidently say referring to the course of events that,

simulation war will have the same meaning as real war in the near future. All of this is really much more dangerous than real war. We believe that, "Second Life", which was created in 2003 and has more than one million active users as a virtual world, can be taken as an obvious example to justify our position. This network, which gradually moves people away from the real world, can play a role of easy and operative psychological effects for "weak" states by "trong" states. The impact of various virtual games on this issue is not negligible as well. For example, it is clear how suicidal the "Blue Whale" game become in recent times. All this shows again that, the "information war" should be analyzed in a practical way than theoretical concept and measures on struggle with it should be taken not only on international, but also national level. Nowadays, countries are able enough to guard secrecy of their information systems electronically, reducing the number of cyber attacks in the political, military and economic spheres. However, perilousness of psychological attacks and harder consequences remained beyond international community. We believe that such psychological attacks can have an adverse effect on all areas (military, political, and economic) as a result of the violation of peoples' morality. The work carried out in our country in this regard should be estimated highly. The work undertaken by the CERT Azerbaijan forms the "immunity" of citizens to protect them from psychological effects.

Conclusions. Pertpertration of traditional crimes are also preferred by the use of ICT in the fast development period of ICT. Today, there is no need to steal money by the use of weapon, but it is possible to become richer in easier ways with the help of technology (bank fraud, etc.). Even forcing a person to commit suicide is possible in the virtual world at distance. Therefore, we consider it appropriate to revise the notion of "cybercrime" in legal sources related to cyber offences. Different classifications of cybercrime can be used in theoretical literature.

Thus, the measure included the elimination of the information ecology, the formation and development of a culture of information security, strengthening of personal data protection measures, abolition of adverse effects of cyberspace on human psychology, should be planned and implemented for the protection and provision of human rights in cyberspace.

References

1. Aliyev A.I., Rzayeva G.A., Ibrahimova A.N., Maharramov B.A., Mammadrzali S.S. Information law. Textbook. Baku: Nurlar, 2019, 448 p.
2. Debra Littlejohn Shinder. Scene of the Cybercrime: Computer Forensics Handbook. Canada: Syngress Publishing, Inc., 2002, 749 p.
3. Fiordalisi E. The Tangled Web: Cross-Border Conflicts of Copyright Law in the Age of Internet Sharing. // Loyola University Chicago International Law Review, 2015, Vol. 12, İssue 2, pp. 197-213.
4. Human Rights in the Global Information Society (Information Revolution and Global Politics). Edited by Rikke Frank Jorgensen, London: The MIT Press Cambridge, Massachusets, 2006, 323 p.
5. John Arquilla and David Ronfeldt. Cyberwar is coming! // National Security Research Division. https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf
6. Martin C. Libicki. What Is Information Warfare? Washington, 1995, 104 p.
7. Official site of CERT Azerbaijan. URL : https://www.cert.az/news/2016/informasiya-tehlukesizliyi-ve-ona-qarsi-yonelmis-hucumlar
8. Recommendations of the Electronic Security Center for the prevention and elimination of the consequences of information security incidents. // Electronic Security Center, 2014. URL : https://www.cert.az/s/u/document/tovsiye.pdf,
9. Understanding Cybercrime: A Guide For Developing Countries. ICT Applications and Cybersecurity Division Policies and Strategies Department, ITU Telecommunication Development Sector Draft April 2009, 225 p.
10. К вопросу о латентности киберпреступлений. URL : https://infourok.ru/statya-k-voprosu-latentnosti-kiberprestupleniy-1460496.html
11. Платошин Ю.А.Сущность латентной преступности. *Право и образование*, 2011, №5, с. 171-176.
12. Рассолов И.М. Право и Интернет: Теоретические проблемы. Москва: Норма, 2009, 383 с.

SUMMARY

In modern society, the Internet has become an integral part of human life. However, not all internet users are law-abiding people. The use of ICTs for various unlawful purposes and its results is one of the most pressing problems of our time, which raises the issue of "cybercrime". In the article were given an explanation of the terms "cybercrime", "cyber war" and "cyber offences", were comparatively analyzed their legal and illegal classification, and were put forward suggestions and recommendations for the prevention of cybercrime.

Keywords: *information security, cyber offences, cybercrime, classification of cybercrimes, cyber war, data, accessibility, confidentiality, completeness.*

УДК 343.79
DOI: 10.31733/2078-3566-2020-2-158-162

Оксана КОРОТЮК©
кандидат юридичних наук
(Дніпропетровський державний університет внутрішніх справ)

ПОВТОРНІСТЬ ЯК КВАЛІФІКУЮЧА ОЗНАКА ЗЛОЧИНІВ, ЩО ПОСЯГАЮТЬ НА ОБ'ЄКТИ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Розкрито особливості повторності як кваліфікуючої ознаки злочинів, які посягають на об'єкти права інтелектуальної власності. Проведений аналіз дозволив дійти висновку, що повторність суспільно небезпечних посягань на об'єкти права інтелектуальної власності має місце у разі: а) учинення окремих суспільно небезпечних діянь щодо одного об'єкта права інтелектуальної власності два чи більше разів (наприклад, повторне незаконне видання того самого твору після продажу попереднього тиражу); б) учинення окремих суспільно небезпечних діянь щодо різних об'єктів права інтелектуальної власності, які визначені в одній статті (частині статті) КК, два чи більше разів (наприклад, учинення незаконного відтворення одного твору, після чого вчинення незаконного відтворення іншого твору); в) учинення двох чи більше різних суспільно небезпечних діянь (тобто діянь, об'єктивна сторона яких є відмінною) щодо об'єктів (об'єкта) права інтелектуальної власності, які визначені (який визначений) в одній статті (частині статті) КК (наприклад, незаконне відтворення твору та його незаконне розповсюдження).

Ключові слова: *кримінально-правова охорона, об'єкти права інтелектуальної власності, повторність, кваліфікуюча ознака, інтелектуальна власність.*

Постановка проблеми. Об'єкти права інтелектуальної власності, що охороняються Кримінальним кодексом України, обумовлюють специфіку компонентів кримінально-правової охорони, що в тому числі стосується кваліфікуючих ознак злочинів, які посягають на об'єкти права інтелектуальної власності.

Аналіз публікацій, у яких започатковано вирішення цієї проблеми. Окремі питання, що стосуються кримінально-правової охорони об'єктів права інтелектуальної власності, а також розкриття ознак злочинів, які посягають на об'єкти права інтелектуальної власності, були розглянуті в роботах П. С. Берзіна [1], Р. А. Волинця [4], А. С. Нерсесяна [10], В. Б. Харченка [13] та інших науковців. Однак комплексного дослідження повторності як кваліфікуючої ознаки злочинів, що посягають на об'єкти права інтелектуальної власності, на сьогодні не було здійснено, тому це питання вбачається актуальним і доцільним.

Метою статті, з огляду на вищезазначене, є з'ясування особливостей повторності як кваліфікуючої ознаки злочинів, які посягають на об'єкти права інтелектуальної власності.

Виклад основного матеріалу. Повторність як кваліфікуюча ознака злочинів неодноразово зазначена законодавцем у кримінально-правових нормах, що стосуються відповідальності за посягання на об'єкти права інтелектуальної власності (ч. 2 ст. 176, ч. 2 ст. 177, ч. 2 ст. 229, ч. 3 ст. 232-1, ч. 2 ст. 232-2 Кримінального кодексу України [7]) (далі – КК). Як бачимо з наведених вище статей, повторність злочинів за ознакою рівня суспільної небезпечності поставлена в законі поряд із вчиненням злочину за попередньою змовою групою осіб (ч. 2 ст. 176, ч. 2 ст. 177, ч. 2 ст. 229, ч. 3 ст. 232-1 КК), із вчиненням злочинного діяння, що завдало матеріальної шкоди у великому розмірі (ч. 2 ст. 176, ч. 3 ст. 177, ч. 2 ст. 229 КК), спричинило тяжкі наслідки (ч. 3 ст. 232-1 КК). Зокрема, такий висновок випливає з єдиної для зазначених діянь санкції, яку цілком справедливо науковці визнають як вираженням ціннісної оцінки об'єкта, що охороняється, так і мірою відповідальності правосуб'єктних осіб [14, с. 63].

Як правильно зазначив В. О. Навроцький, за чинним законодавством ознакою складу злочину повторність визнається тоді, коли вчинення наступного злочину якось

© Коротюк О.В., 2020
ORCID iD : https://orcid.org/0000-0003-0081-3901
ovk@korotyuk.com