Scientific News of Azerbaijan State Academy of Physical Education and Sport
Sport Science Journal vol. 6, № 1, 2024, pp. 87-91.

MÜASİR DÖVRDƏ KİBERCİNAYƏTKARLIQ

M.Ş. Şirinov[1a], A.Ə. Bədirxanov[1,b]

[1] *Azərbaycan Dövlət Bədən Tərbiyəsi və İdman Akademiyası*
[a] mubariz.shirinov@sport.edu.az, orcid.org/0009-0007-5294-5697
[b] adil.badirkhanov@sport.edu.az, orcid.org/0009-0009-2914-9398

Nəşr tarixi
Qəbul edilib: 29 yanvar 2024
Dərc olunub: 25 mart 2024

Annotasiya. XXI əsrdə elmi-texniki tərəqqinin yeni – informasiya inqilabı adlanan mərhələsi həyat səviyyəsinin və sosial rifahın yüksəldilməsinə yönələn nəticələri ilə yanaşı, milli, hərbi və siyasi, xüsusilə də sosial təhlükəsizliyə təhdid olan yeni cinayətkarlıq formalarının inkişafı və genişlənməsinə də təkan vermişdir. Hazırda ölkələrin kibersisteminə qeyri-qanuni şəkildə daxil olmaq, sistemi istismar etmək və ya pozmaq fəaliyyəti milli təhlükəsizlik üçün təhdid amilinə çevrilmişdir. İnformasiyanın və ya elektron cihazların, proseslərin, məlumatların emalı zamanı istifadə edilən texnologiyalar sisteminə qəsdən və ya icazəsiz giriş, onun manipulyasiyası və ya məhv edilməsi məqsədilə həyat keçirilən kiberhücumlar əqli mülkiyyət itkilərinin iki dəfə artmasına səbəb olmuşdur. Elm və texnologiyalar insanların həyat tərzinin yaxşılaşdırılmasına yönəlmişdir, lakin informasiya texnologiyalarının sürəti həyat mobilliyini artırmış, təhlükəsizlik baxımından yeni narahatlıqlar yaratmışdır. XXI əsr yeni dünya nizamının formalaşması insanların rifahına və ümumilikdə mövcud olmasına təhlükə yaradan cinayətkarlığın yeni formalarda təzahürünə gətirib çıxarmışdır. Hazırda klassik oğurluq və fırıldaqçılıq kimi cinayət əməlləri fiziki təmas və ya qurbanla eyni yerdə olmadan virtual mümkünlük qazanmışdır. Son onilliklərdə nəinki hər il, hətta hər ay yeni formaları ortaya çıxan kibercinayətlərin bitkin və əhatəli tərifi bu gün üçün mövcud olsa belə, natamam xarakterli olardı. Bununla yanaşı, kibertəhdid və cinayətlərin çoxsaylı, dar və geniş mənada izah və tərifləri mövcuddur.

Açar sözlər: *kibercinayətkarlıq, definisiya, kibermәkan, kibertəhlükəsizlik, kiberhücum, kibertəhdid, informasiya müharibəsi, informasiya əməliyyatları.*

XXI əsrdə elmi-texniki tərəqqinin yeni – informasiya inqilabı adlanan mərhələsi həyat səviyyəsinin və sosial rifahın yüksəldilməsinə yönələn nəticələri ilə yanaşı, milli, hərbi və siyasi, xüsusilə də sosial təhlükəsizliyə təhdid olan yeni cinayətkarlıq formalarının inkişafı və genişlənməsinə də təkan vermişdir. Hazırda ölkələrin kibersisteminə qeyri-qanuni şəkildə daxil olmaq, sistemi istismar etmək və ya pozmaq fəaliyyəti milli təhlükəsizlik üçün təhdid amilinə çevrilmişdir. İnformasiyanın və ya elektron cihazların, proseslərin, məlumatların emalı zamanı istifadə edilən texnologiyalar sisteminə qəsdən və ya icazəsiz giriş, onun manipulyasiyası və ya məhv edilməsi məqsədilə həyat keçirilən kiberhücumlar əqli mülkiyyət itkilərinin iki dəfə artmasına səbəb olmuşdur. Elm və texnologiyalar insanların həyat tərzinin yaxşılaşdırılmasına yönəlmişdir, lakin informasiya texnologiyalarının sürəti həyat mobilliyini artırmış, təhlükəsizlik baxımından yeni narahatlıqlar yaratmışdır. XXI əsr yeni dünya nizamının formalaşması insanların rifahına və ümumilikdə mövcud olmasına təhlükə yaradan cinayətkarlığın yeni formalarda təzahürünə gətirib çıxarmışdır. Hazırda klassik oğurluq və fırıldaqçılıq kimi cinayət əməlləri fiziki təmas və ya qurbanla eyni yerdə olmadan virtual mümkünlük qazanmışdır [1].

Son onilliklərdə nəinki hər il, hətta hər ay yeni formaları ortaya çıxan kibercinayətlərin bitkin və əhatəli tərifi bu gün üçün mövcud olsa belə, natamam xarakterli olardı. Bununla yanaşı, kibertəhdid və cinayətlərin çoxsaylı, dar və geniş mənada izah və tərifləri mövcuddur. Kibercinayətkarlıq kompüterin,

kompüter şəbəkəsinin və ya şəbəkə qurğusunun istifadə edildiyi və ya hücuma məruz qaldığı cinayət fəaliyyətidir. Kiberhücumların əksəriyyəti kibercinayətkarlar və ya hakerlər tərəfindən maliyyə mənfəəti əldə etmək üçün həyata keçirilir. Bununla belə, kiberhücumların məqsədi, həm də şəxsi və ya siyasi səbəblərdən kompüterlərin və ya şəbəkələrin məqsədyönlü şəkildə sıradan çıxarılmasıdır. Kibercinayətkarlıq yeni başlayan hakerlərdən tutmuş qabaqcıl texnikalardan istifadə edən və texnologiyaya yaxşı bələd olan sıx şəbəkələşmiş dəstələrə qədər müxtəlif şəxslər və təşkilatlar tərəfindən törədilir. Hazırda dünyada kibercinayətlər törədən çoxsaylı belə şəbəkələr mövcuddur [2].

Başqa sözlə, yaşadığımız real dünyada: internet üzərindən virtual məkanda təşkil oluna və insana qarşı yönəldilə bilən istənilən cinayət – kibercinayət adlanır. Ümumilikdə şəxsi məlumatların oğurlanması, terror aktlarının törədilməsi, elektron əmlakın qeyri-qanuni olaraq ələ keçirilməsi (məsələn, elektron, rəqəmsal quldurluq/piratlıq), qeyri-qanuni köçürmə əməliyyatları, informasiya əldə etmək üçün özünü "etibarlı, səlahiyyətli" bir şəxs kimi təqdim etmək (fırıldaqçılıq), yaxud zərərli və ya qanunsuz informasiya (spam) əks etdirən irihəcmli elektron məktublar göndərmək və s. kibercinayət hesab edilir. İnternet/informasiya sistemlərinə qanunsuz daxilolma, müdaxilə, habelə digər formalarda informasiya təhlükəsizliyinin pozulmasına yönəldiyi ehtimal edilən səylər isə kibertəhdid kimi səciyyələndirilir [4].

Kibercinayətkarlıq hesab edilir:

– viruslar və ya digər zərərli proqramlar vasitəsilə kompüterlərə hücum edərək cinayət törədilməsi;
– başqa cinayətlər törətmək məqsədilə kompüterlərdən və digər elektron resurslardan istifadə. Kibercinayətkarlıq getdikcə artan qlobal problemdir. Təsadüfi deyil ki, Dünya İqtisadi Forumunun (WEForum) ekspertləri 2021-ci ili dünyada "kiberpandemiya ili" adlandırmışlar: bəşəriyyət "kiberpandemiya"nın ortasındadır. COVID-19 məsafədən işləməyə keçidi sürətləndirdi ki, bu da hücum məqsədilə istifadə olunan proqram təminatının icrasını asanlaşdırdı ("ransomware" hücumları görünməmiş sürətlə artmaqda davam edir) [1]. Beləliklə, hazırda hər kəs - ağıllı telefon istifadə edən şəxslər, kiçik biznes, "Fortuna 500" ən qabaqcıl innovasiya reytinqi siyahısına daxil olan qlobal şirkətlər, eləcə də kibertəhlükəsizlik üzrə ayrıca mütəxəssislər kibercinayətlərdən xəbərdar olmalıdır. İnternet bir tərəfdən dünyaya indiyədək görünməmiş faydalı imkanlar verir, digər tərəfdən görünməmiş ziyanlara yol açır. Texnologiyalardan sui-istifadə edən kibercinayətkarlar həm bütöv biznes sahələrini, həm də insanların şəxsi həyatını məhv edir. Dünya ölkələri, beynəlxalq təşkilatlar kibercinayətkarları dayandırmaq və kibertəhlükəsizliyi təmin etmək üçün mübarizə aparır. Qlobal cəmiyyətdə əhalinin yarısından çoxu, təqribən üçdə ikisi internet bağlantısına, 20%-i isə sosial şəbəkələrə üzvdür. Məlumdur ki, hazırda dünya əhalisinin 85%-i mobil cihazlardan istifadə edir, 15% insan mobil telefonların ticarəti ilə məşğuldur. Təqdim edilən statistik göstəricilər bəşəriyyətin informasiya texnologiyalarından qeyri-adi asılılığa malik olduğunu nümayiş etdirir. İnformasiya texnologiyalarından, xüsusən də internetdən beynəlxalq asılılıq davamlı şəkildə yüksəlir. Tədqiqatçılar güman edirlər ki, qlobal şəbəkədə gündəlik 294 milyard e-poçt mesajı göndərilir və 24 saat müddətində 168 milyon DVD məlumatı istehsal edilir. Youtube serverlərinə gündəlik 864.000 saat video yüklənir, Netflix istifadəçiləri gündə 22 milyon saat TV və ya film izləyirlər [2,3,4].

Avtomatlaşdırılmış idarəetmə sistemlərinin kiber təhlükəsizliyi – Avtomatlaşdırılmış idarəetmə sistemlərində (AİS) kompüter şəbəkəsi və verilənlər bazası kimi müasir informasiya texnologiyalarının (İT) istifadəsi zamanı informasiyanın dəyəri artır, belə ki, informasiya məlumatlanma dərəcəsini artırmağa, müxtəlifsəviyyəli komandanlıq, hərbi idarəetmə orqanları və kəşfiyyat arasında qarşılıqlı əlaqəni yaxşılaşdırmağa və bununla da öz informasiya üstünlüyünü reallaşdırmağa imkan

verir. İT-nin inkişafı və onlar əsasında yaradılanların AİS-ə tətbiqi, qoşunların sürətlə informasiya yüklü silah, hərbi texnika (HT), yüksək dəqiqlikliyə malik kəşfiyyat və məhvetmə vasitələri ilə təmin edilməsi, informasiya mübarizəsi silahlı qüvvələrin ümumi qəbul edilmiş və ənənəvi idarəetmə modelində köklü dəyişikliklərə səbəb oldu. Əsas tərkib hissəsi informasiya və texnoloji üstünlüyün nailiyyətləri olan əməliyyatlar ön plana çıxdı. Bu tendensiyalar özünü NATO-nun Balkanlar, Əfqanıstan və İraqda apardığı hərbi əməliyyatlar zamanı daha aydın şəkildə göstərdi [9]. Hazırda NATO-ya üzv ölkələr, ÇXR və Rusiya kimi böyük hərbi potensiala malik dövlətlər özünün kiber təhlükəsizliyinin təmin edilməsi probleminə çox ciddi yanaşırlar. Sözügedən oblastda liderlik, sözsüz ki, informasiya qarşıdurması strategiyasının əsaslarını hələ 1992-ci ildə irəli sürmüş ABŞ-a məxsusdur [5-8].

ABŞ-ın Silahlı Qüvvələrinin qərargah rəisləri komitəsi tərəfindən təsdiq edilmiş "İnformasiya əməliyyatları" sənədində Amerika hərbi rəhbərliyinin informasiya əməliyyatlarının hazırlanması, həyata keçirilməsi, informasiya qarşıdurmasının məqsədi və əsas prinsiplərinə dair baxışları, həmçinin belə əməliyyatların sülh və müharibə şəraitində hazırlanmasına cavabdeh olan vəzifəli şəxslərin vəzifə borcları göstərilmişdir [10]. Sənəddən göründüyü kimi, informasiya əməliyyatları düşmən tərəfin informasiya - kommunikasiya şəbəkələrinin və kompüter sistemlərinin müdafiəsini, eyni zamanda düzgün qərar qəbul etməsini çətinləşdirmək və yaxud tamamilə mümkünsüz etmək üçün maddi və mənəvi resurslarına təsir göstərən kompleks tədbirləri əhatə edir. Belə əməliyyatlar, əsasən, 5 tərkib hissəsindən ibarətdir [11]:

– radioelektron mübarizə (electronic warfare);
– psixoloji əməliyyatlar (psychological operations);
– informasiya-kommunikasiya şəbəkələrində əməliyyatlar (computer network operations);
– hərbi dezinformasiya (military deception);
– operativ təhlükəsizlik (operations security).

Sülh və müharibə şəraitində informasiya əməliyyatlarının uğurlu başa çatması üçün vacib olan köməkçi elementləri də təyin olunmuşdur:

– informasiya dayanıqlılığı (information assurance);
– fiziki təsir (physical attack);
– əks-kəşfiyyat (counter intelligence);
– fiziki təhlükəsizlik (physical security);
– verilənlərin toplanması və istifadə olunması (combat camera);
– ictimaiyyətlə əlaqə (public affairs);
– mülki - hərbi əməliyyatlar (civil - military operations);
– ictimai diplomatiyanın Müdafiə Nazirliyinin strukturları tərəfindən dəstəklənməsi (defense support to public diplomacy) [12].

ƏDƏBİYYAT

1. *Protecting critical infrastructure from a cyber pandemic*: [Electronic resource]. October 20, 2021. URL: https://www.weforum.org/agenda/2021/10/protecting-critical-infrastructure-from-cyberpandemic/
2. *Two-thirds of the world's population are now connected by mobile devices:* [Electronic resource]. September 19, 2017. 6:31 PM GMT+4. URL: https://www.businessinsider.com/world-population-mobile-devices-2017-9.
3. **Məcidli, S.T.** *Kibercinayətlər*. S.T.Məcidli. Bakı, 2019, 314 s.
4. *The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub.* Tallim 10132, Estonia: [Electronic resource]. URL: https://ccdcoe.org/
5. **Корсаков, Г.Б.** *Роль информационного оружия в военно-политической стратегии США*. США и Канада: экономика, политика, культура, 2012, №1, с. 39-60.
6. **Пашков В.** *Информационная безопасность США*. Зарубежное военное обозрение, 2010, №10, с. 3-13.

7. **Роговский Е.А.** *Политика США по обеспечению безопасности киберпространства*. США и Канада: экономика, политика, культура, 2012, № 6, с. 3-22.
8. **Храмчихин А.А.** *Стратегические концепции Китая в геополитическом аспекте*. Международные научные исследования, 2011, № 3-4, с. 18-23.
9. **Бобров А.** *Информационная война: От листовки до твиттера*. Зарубежное военное обозрение, 2013, №1, с. 20-27.
10. AFDD 3-12, Cyberspace Operations, USAF, 2010, 60 p.
11. AFDD 3-13, Information Operations, USAF, 2011, 65 p.
12. AFPD 10-7, Information Operations, USAF, 2006, 29 p.

КИБЕРПРЕСТУПНОСТЬ В НАШЕ ВРЕМЯ

М.Ш. Ширинов[1a], А.А. Бадирханов[1,b]

[1] *Азербайджанская Государственная Академия Физической Культуры и Спорта*
[a] mubariz.shirinov@sport.edu.az, orcid.org/0009-0007-5294-5697
[b] adil.badirkhanov@sport.edu.az, orcid.org/0009-0009-2914-9398

Аннотация. В XXI веке наступил новый этап научно-технического прогресса, получивший название информационной революции, наряду с ее результатами, направленными на повышение уровня жизни и общественного благосостояния, это также стимулировало развитие и распространение новых форм преступности, угрожающих национальной, военной, политическое и особенно социаль-ное обеспечение. В настоящее время незаконное проникновение в киберсистему стран, ее эксплуатация или разрушение стало фактором угрозы национальной безопасности. Преднамеренный или несанкционированный доступ к системе информации или электронным устройствам, процессам и технологиям, используемым при обработке данных, кибератаки, осуществляемые с целью манипулирования ими или уничтожения, привели к двукратному увеличению потерь интеллектуальной собственности. Наука и технологии направлены на улучшение образа жизни людей, но скорость информационных технологий увеличила мобильность жизни и создала новые проблемы безопасности. Формирование нового мирового порядка XXI века привело к проявлению преступности в новых формах, что ставит под угрозу благополучие и общее существование людей. В наши дни классические преступления, такие как кража и мошенничество, стали практически возможными без физического контакта или нахождения в одном месте с жертвой. Исчерпывающее и всеобъемлющее определение киберпреступности, которое появлялось не только каждый год, но и каждый месяц в последние десятилетия, было бы неполным, даже если бы оно существовало сегодня. Кроме того, существует множество узких и широких объяснений и определений киберугроз и преступлений.

Ключевые слова: *киберпреступность, определение, киберпространство, кибербезопасность, кибератака, киберугроза, информационная война, информационные операции.*

CYBERCRIME IN MODERN TIMES

M.SH. Shirinov[1a], A.A. Badirkhanov[1,b]

[1] *Azerbaijan State Academy of Physical Education and Sport*
[a] mubariz.shirinov@sport.edu.az, orcid.org/0009-0007-5294-5697
[b] adil.badirkhanov@sport.edu.az, orcid.org/0009-0009-2914-9398

Annotation. In the 21st century, the new stage of scientific and technical progress called the information revolution, along with its results aimed at improving the standard of living and social welfare, has also stimulated the development and expansion of new forms of crime that threaten national, military, political, and especially social security. At present, illegally entering the cyber system of countries, exploiting or disrupting the system has become a threat factor for national security. Intentional or unauthorized access to the system of information or electronic devices, processes, and technologies used during data processing, cyber-attacks carried out for the purpose of its manipulation or destruction caused a doubling of intellectual property losses. Science and technology are aimed at improving people's lifestyle, but the speed of information technology has increased the mobility of life and created new security concerns. The formation of the new world order of the 21st century has led to the manifestation of criminality in new forms, which threatens the well-being and general existence of people. Nowadays, classic crimes such as theft and fraud have gained a virtual possibility without physical contact or being in the same place with the victim. An exhaustive and comprehensive definition of cybercrime, which has emerged not only every year, but even every month, in recent decades, would be incomplete even if it existed today. In addition, there are numerous, narrow and broad explanations and definitions of cyber threats and crimes.

Keywords: *cybercrime, definition, cyberspace, cyber security, cyber attack, cyber threat, information warfare, information operations.*