UOT 34:343.2 Cinayət hüququ

ŞÖHLƏT KƏRİMOV

Milli Aviasiya Akademiyasının "Hüquq" kafedrasının dosenti,hüquq üzrə fəlsəfə doktoru

ŞAİR ABDURAHMANOV

Milli Aviasiya Akademiyasının "Hüquq" kafedrasının baş müəllimi

KİBERCİNAYƏTKARLIQ VƏ ONUNLA CİNAYƏT-HÜQUQİ MÜBARİZƏ

Açar sözlər: rəqəmsal, kompüter cinayətləri, süni intellekt, kibercinayətkarlıq, kiberdələduzluq, xaker hücumu, transmilli cinayət, internet şəbəkəsi, informasiya texnologiyaları
Keywords: digital, computer crimes, artificial intelligence, cybercrime, cyberfraud, hacker attack, transnational crime, Internet network, information technology
Anahtar kelimeler: dijital, bilgisayar suçları, yapay zeka, siber suçlar, siber dolandırıcılık, hacker saldırısı, ulusötesi suç, internet ağı, bilgi teknolojisi

Beynəlxalq Kriminologiya Cəmiyyətinin verdiyi məlumata görə, elm və texnologiyanın inkişafı sahəsində iqtisadi cəhətdən inkişaf etmiş ölkələrdə transmilli cinayətlərin bir növü olan kibercinayətkarlığın səviyyəsi ildən-ilə artmaqda davam edir. Buna səbəb rəqəmsal texnologiyanın inkişafı ilə bağlı süni intellektin tətbiq olunmasıdır.

Süni intellekt insan davranışını və ya düşüncəsini təqlid edən və xüsusi problemləri həll etmək üçün öyrədilə bilən maşınla nümayiş etdirilən intellektdir. Süni intellekt maşın və dərin öyrənmə üsullarının birləşməsidir. Böyük miqdarda məlumatlardan istifadə edərək öyrədilmiş süni intellekt modelləri ağıllı qərarlar qəbul etməyə qadirdir. [1, s.18]

Bu gün rəqəmsal texnologiyanın inkişafı həyatımızı nə qədər asanlaşdırsa da, digər tərəfdən bir o qədər çətinləşdirir. Belə ki, son vaxtlar kiberdələduzluq ən geniş yayılmış cinayətlərdən biri hesab olunur. Əhalinin müəyyən bir qismi kibertəhlükəsizlik qaydalarını bilmədiyi və ya əməl etmədiyi üçün kiberdələduzların qurbanına çevrilir.

Kibercinayətkarlıq problemi bir dövlət sərhədləri ilə məhdudlaşmadığına və qlobal xarakter daşıdığına görə onunla mübarizə aparmaq üçün vahid beynəlxalq standartların işlənib hazırlanması günün tələbidir.

Kiberdələduzluqla bağlı 2024-cü ildə mətbuatda və KİV-də verilən bir neçə rəsmi statistikaya nəzər salaq.

Azərbaycan Dövlət Televiziyasında 29.07.2024-cü il tarixli "Xəbərlər" proqramında göstərilir ki, DİN-in Kibercinayətlərlə Mübarizə Baş İdarəsi 4 nəfərdən ibarət kiberşəbəkəni müəyyən edərək ələ keçirib. Bu cinayətkar şəbəkənin üzvləri kiberdələduzluq yolu ilə 400 nəfərə yaxın insanın bank hesablarından yarım milyon manatdan çox pul vəsaitini ələ keçiriblər.

Azərbaycan Dövlət Televiziyasında 02.08.2024-cü il tarixli "Xəbərlər" proqramında qeyd edilir ki, universitetlərdən birində müəllim işləyən qadının bank kartından kibercinayət yolu ilə 52 min manat pul çıxarılıb.

"ARB" televiziya kanalının 29.09.2024-cü il tarixli "Xəbərlər" proqramında qeyd edilir ki, DİN-in kibercinayətkarlıqla Baş Mübarizə İdarəsi tərəfindən H. və S. adlı şəxslərin barəsində həbs qətimkan tədbiri həyata keçirilib. Onlar "farmoniya.com" saytı açıb dələduzluq yolu ilə maliyyə piramidası yaradıblar. 18 mindən çox adam bu fırıldaqçıların toruna düşüb. Bu fırıldaqçılar əhalinin 700 min manatdan çox pulunu dələduzluq yolu ilə ələ keçirmişlər.

Digər bir maliyyə piramidasında əhalini

aldadaraq 5 milyon manatdan çox pul ələ keçirilib. Qrupun başçısı tutulub, digərlərinin axtarışı barədə əməliyyat tədbirləri davam edir. Bu cür misallar yüzlərlədir. Bəzi insanlar belə dələduzların qurbanı olur. Ona görə də bank hesablarını, bankomat kartlarının nömrəsini heç kimə vermək olmaz.

"Kibercinayətkarlıq haqqında Budapeşt Konvensiyası" 4 hissə və 48 maddədən ibarətdir. Bu konvensiya kibercinayətkarlıqla mübarizədə mühüm rol oynayır. Konvensiyanın 13-cü maddəsi kibercinayətlərə görə sanksiya və tədbirləri nəzərdə tutur [2].

Kibercinayətlər transmilli hesab olunduğu üçün onlarla mübarizədə İnterpol və Europol kimi beynəlxalq təşkilatlar mühüm rol oynayır. Belə ki, bu təşkilatlar kibercinayətkarlıqla mübarizədə dövlətlər arasında həm məlumat mübadiləsi aparır, həm də birgə əməliyyatlarda iştirak edir.

Bəzi alimlər "cinayətin kökünü kəsməyi" bir məqsəd kimi qarşıya qoyurlar. Bu, mümkün deyildir. E.Dürkheyn göstərir ki, cinayətkarlıq normal bir hadisədir. Çünki onsuz cəmiyyətin varlığı tamamilə mümkün deyil. Cinayətkarlıq zəruridir; o, hər bir sosial həyatın əsas şərtləri ilə sıx əlaqəli olmalıdır [3, s.15].

Beləliklə, həqiqət ondan ibarətdir ki, cinayətkarlıq problemini heç bir sosial-siyasi sistem həll edə bilməmişdir [4, s.131]. Çezere Bekkaria yazırdı ki, cinayətin qarşısını almaq cəzalandırmaqdan yaxşıdır [5, s.119].

Kibercinayətkarlıqda əsas məqsəd zəhmətsiz gəlir əldə etməkdir. Kibercinayətkarlıq digər cinayətlərdən onunla fərqlənir ki, bu cinayətləri törədənlər heç də savadsız, avara deyillər, onların çoxu yüksək intellektə malik olan, savadlı, "ağköynəkli", "boynu qalstuklu" şəxslərdir. Kibercinayətləri törədən şəxslərin internet şəbəkəsi ilə işləmələri və kompüter bacarıqları mükəmməl olur [6, s.63-64].

Kibercinayətkarlığın tarixi nisbətən yenidir. Prof.Y.S.Romaşev qeyd edir ki, XX əsrin 80-90-cı illərinə qədər kompüter texnologiyasının istifadəsi ilə bağlı cinayətlərin payı çox da böyük olmamışdır. Lakin zəhmətsiz qazanc məqsədilə və əyləncə naminə kompüter şəbəkələrindən qanunsuz istifadə, uşaq pornoqrafiyasının yayılması, kompüter və informasiya sistemlərinin dağıdılması təhlükəsi, habelə kompüter şəbəkəsindən dələduzluq məqsədilə istifadə olunması kompüter cinayətlərinin adi formalarından hesab olunur [7, s.253].

Dünyanın əksər ölkələrində kibercinayətkarlıqla mübarizə aparmaq üçün cinayət hüququnun müəyyən normalarına istinad edilir. Belə normalar hər bir ölkənin qanunvericiliyində kibercinayətlərin qarşısını almaq və bu cinayətləri törədən şəxsləri məsuliyyətə cəlb etmək məqsədi daşıyır.

Hüquq ədəbiyyatında kibercinayətə belə anlayış verilir: informasiya və telekommunikasiya texnologiyalarından istifadə etməklə törədilən təqsirli, ictimai-təhlükəli, cinayət məsuliyyəti nəzərdə tutulan əməl kibercinayət hesab olunur. İnternet şəbəkəsi və kompüterlər müasir cəmiyyətdə adi bir əşya kimi, cisim kimi qarşılanır. Lakin bu yüksək texnologiya cinayətin yeni növünün - kibercinayətkarlığın yaranmasına gətirib çıxarmışdır. Qeyd etmək lazımdır ki, getdikcə insanlar gündən-günə inkişaf edən texnologiyadan daha çox asılı vəziyyətə düşürlər. Elə buna görə də deyə bilərik ki, kibercinayətkarlıq bu gün dünyada ən aktual mövzulardan biridir.

Kibercinayətkarlıq - kompüter sistemlərinə və ya digər informasiya texnologiyaları şəbəkələrinə, cəmiyyətin informasiya təhlükəsizliyinə və kibermaraqlarına əhəmiyyətli ziyanın vurulması ilə xarakterizə edilən hərəkət və hərəkətsizlikdən ibarət transmilli cinayət əməlidir [8,s.128]. İnformasiya texnologiyaları və internet vasitəsilə törədilən kibercinayətkarlıq latent cinayətkarlıqdır.

Kibercinayətlərin real həyatda törədilmə səbəbləri müxtəlif olsa da, bu sahədə tədqiqat aparan alimlərin fikirləri qismən də olsa üst-üstə düşür:

- kompüterdən əylənmək üçün istifadə edilməsi - bəzi gənclər və xakerlər internetdən və kompüterlərdən əyləncə kimi istifadə edirlər. Bu zaman başqa şəxslərin şəbəkələrinə müdaxilə edirlər. Öz istedadlarını göstərmək üçün başqalarının veb səhifələrini korlayır və viruslar göndərirlər. Əslində onların məqsədi

ziyan vurmaq olmasa da, ancaq hərəkətləri ilə təbii ki, başqalarına zərər yetirirlər.

- şöhrət hissi - rəqabət aparmaq, tez bir zamanda populyar olmaq və bunun nəticəsində müxtəlif nüfuzlu şirkətlərin mühafizəçisi statını əldə etmək və s. cinayət törətmək üçün səbəb ola bilər [8, s.131].

- pul qazanmaq istəyi - bu hal kibercinayətlərin başlaması üçün əsas səbəblərdən biridir. Respublikamızda kibercinayətlərin əsas törədilmə səbəbi məhz budur. Kiberdələduzlar və ya xakerlər vətəndaşların bank hesablarının və ya bankomat kartlarının nömrəsini ələ keçirməklə bu cinayəti törədirlər.

- emosiya (qəzəb) intiqam - bu elə bir emosional vəziyyətdir ki, burada pul qazanmaq yox, kin, qəzəb, hirs, sevgi intiqamı kimi məsələlər ön plana çıxır.

- cinsi impulslar - belə qrupa daxil olanlar, əsasən, uşaq pornoqrafiyasını yayanlar və istifadə edən şəxslərdir. Uşaq pornoqrafiyasını yayan şəxslər kommersiya məqsədi də güdə bilərlər.

- siyasi və dini məqsədlər - belə şəxslər internetdən öz məqsədlərinə çatmaq üçün təbliğat vasitəsi kimi istifadə edirlər. Siyasi mənsubiyyətlər və dini inanclar bəzən kibercinayətlərin törədilməsinə səbəb olur.

Kibercinayətkarlığın mahiyyəti özünü informasiya texnologiyaları və internet şəbəkələri vasitəsi ilə törədilən aşağıdakı cinayətlərdə göstərir:

1. Məlumatların oğurlanması və sızdırılması - bu özünü şəxsi və ya kommersiya

məlumatlarının qanunsuz əldə edilməsi və ya yayılmasında göstərir.

2. Fırıldaqçılıq və maliyyə dələduzluğu - bu ən geniş yayılmış kibercinayətlərin növlərindəndir. Belə hallar ən çox internet vasitəsi ilə bank hesablarına, bank kartlarına və digər maliyyə sistemlərinə hücumlarda özünü göstərir. Statistikaya əsasən, dünya üzrə böyük miqyaslı kiberhücumlar nəticəsində ölkələrə dəyən ümumi zərərin miqdarı yüksəkdir. Bu statistikaya əsasən, 2025-ci ildə proqnoz olunan zərərin həcmi 10,5 trilyon ABŞ dollarıdır, bu isə hər dəqiqədə 20 milyon ABŞ dolları həcmində zərər deməkdir [9, s.8].

3. Xaker hücumları - xakerlər kompüter texnologiyaları sahəsində yüksək səviyyədə biliyə malik olan və kompüter sistemlərində zəif cəhətləri tapmaq üçün kompüter başında saatlarla vaxt keçirən savadlı şəxslərdir. Xakerlər özləri də bir neçə kateqoriyaya bölünür:

- Piratlar- bunlar müəyyən texniki təcrübəyə malik qeyri-peşəkar şəxslərdir.
- Brauzerlər - digərlərinin kompüterlərinə, sistemlərinə və informasiya resurslarına qeyri-qanuni giriş əldə edə bilən orta səviyyəli texniki imkanlara malik olan şəxslərdir.
- Krekerlər - bunlar kibercinayətkarlıq sahəsində ən yüksək texniki imkanlara malik olan oğrular qrupudur. Böyük ziyan vuran ən müxtəlif cinayətləri məhz bu "krekerlər" həyata keçirirlər.

4. Şantaj və fişinq - bu növ cinayətlər aldatma yolu ilə internet istifadəçilərinin şəxsi məlumatlarını ələ keçirmək məqsədilə törədilir.

5. Zərərli proqramlar - bu sahədə kompüter virusları, troyanlar və fidyə proqramları vasitəsi ilə sistemlərə zərər yetirilməsi nəzərdə tutulur.

6. Uşaq istismarı və qeyri-qanuni məzmunlu məlumatların yayılması - burada qeyri-qanuni məzmunlu materialların internet vasitəsi ilə yayılmasından söhbət gedir.

7. Dövlət və hökumət sistemlərinə hücumlar - artıq 50 ildən artıqdır dünyanın bir çox sivil ölkələrində elektron hökumətlər və rəqəmsal dövlətlər fəaliyyət göstərir. Azərbaycan Respublikası son illərdə rəqəmsal informasiya sahəsində əhəmiyyətli addımlar ataraq elektron hökumətdən rəqəmsal dövlətə keçid istiqamətində uğurlu nəticələr əldə edib. Bu transformasiya ölkənin iqtisadiyyatının rəqəmsallaşdırılması, vətəndaş məmnunluğunun artırılması və dövlət idarəçiliyinin yüksəldilməsi kimi mühüm məqsədlərə xidmət edir.

Rəqəmsal texnologiyaların geniş tətbiq edildiyi zamanda informasiya texnologiyalarından istifadə ilə əlaqədar insanların, dövlət və özəl qurumların, bir sözlə, hər kəsin kiber hücumlara məruz qalması təhlükəsi vardır. Məsələnin ciddiliyi həm də onunla əlaqəlidir ki, bir ölkənin ərazisində kibercinayətlərin törədilməsi üçün fiziki olaraq həmin ölkənin ərazisində olmağa

ehtiyac yoxdur [9, s.5].

Bütün dövlətlərdə kibertəhlükəsizlik kompüterlərin, serverlərin, elektron sistemlərin, mobil qurğuların, şəbəkələrin və məlumatların ziyanverici hücumlardan qorunması deməkdir. Bu, informasiya texnologiyaları təhlükəsizliyi hesab olunur. Bu təhlükəsizlik bir neçə kateqoriyaya bölünür:

- Şəbəkə təhlükəsizliyi;
- Proqram təhlükəsizliyi;
- İnformasiya təhlükəsizliyi;
- Əməliyyatların təhlükəsizliyi;
- Məlumat itkisinin qarşısının alınması;
- Müdaxiləni aşkar edən sistemlər və ya müdaxilənin qarşısını alan sistemlər;
- Eyniləşdirmə və girişin idarə olunması;
- Şifrələmə;
- Antivirus;
- Qəza hallarında bərpa və işin davamlılığı;
- Son istifadəçilərin maarifləndirilməsi [9, s.11].

Kibercinayətkarların məqsədlərindən asılı olaraq bir neçə tipləri mövcuddur. Belə ki, ilkin olaraq kiberdələduzları göstərə bilərik. Bunlar əsasən internet vasitəsilə şübhəli linklər göndərərək insanların şəxsi məlumatlarını və bank kartı məlumatlarını ələ keçirmək məqsədi güdür.

Hədə-qorxu ilə tələb edənlər ikinci tip kibercinayətkarlar hesab edilir. Bunlar insanların etibarını qazanaraq onlardan müəyyən məlumatları əldə edirlər və sonradan bu məlumatlardan pul, gəlir və yaxud müəyyən hərəkətlərin edilməsi üçün onları şantaj edirlər.

Ən geniş yayılmış tiplərdən biri də uşaq pornoqrafiyasını yayanlardır. Bu tipi yayanlar çox vaxt "dark web" vasitəsi ilə şəxsiyyətlərini gizlədirlər, pul qazanmaq üçün uşaq pornoqrafiyası materiallarını həm yayır, həm də satmaqla məşğul olurlar.

Xakerlər - şəxslərin kompüter və şəbəkələrini dağıdaraq ələ keçirmək üçün kompüter soxulcanlarından və viruslarından istifadə edirlər.

Kibercinayətkarların digər bir tipi də təbliğatçılardır. Onlar öz məqsədlərinə çatmaq üçün internet şəbəkəsindən siyasi və ya dini təbliğatı həyata keçirmək üçün istifadə edirlər.

Kibercinayətkarların bir tipi də başqalarının şərəf və ləyaqətini alçaldılması ilə məşğul olan şəxslərdir. Bunlar əsasən başqa ölkələrdə yerləşir və sosial şəbəkələr vasitəsi ilə təhqiramiz ifadələr işlədirlər.

Rəsmi statistikaya əsasən, deyə bilərik ki, respublikamızda kibercinayətkarlıq gündən-günə artan tendensiya ilə müşahidə olunur. Hal-hazırda kibercinayətkarlığa qarşı mübarizədə bir neçə metoddan istifadə olunur:

- Qanunvericilik və kibersiyasətlərin gücləndirilməsi metodu. Buna uyğun olaraq müvafiq qanunların qəbul edilməsi və cəza tədbirlərinin görülməsi;
- Ölkələrlə beynəlxalq əməkdaşlıq. Kibercinayətkarlığın qarşısının alınması və cinayətkarları izləmək üçün informasiya mübadiləsinin həyata keçirilməsi;
- "Firewal" və antivirus proqramları kibertəhlükələrin qarşısınının alınmasında və sistemlərin təhlükəsizliyinin təmin edilməsi;
- Məlumatların şifrələnməsi zamanı kibercinayətkarların məlumatları oğurlamaq imkanlarının qarşısının alınması;
- Təlim və məlumatlandırma metoduna görə, bütün işçilər kibertəhlükəsizlik sahəsində maarifləndirilməsi, həm də onların bu sahədə savadlandırılması;
- Güclü parol və autentifikasiya metodu vasitəsi ilə kibercinayətkarlığın qarşısının alınması;
- Monitorinq və idarəetmə metodu təhlükəsizlik sistemlərinin və şəbəkələrin daimi monitorinqinin keçirilməsi.

Qeyd olunan bu metodlar kibercinayətlərin qarşısının alınmasına, sayının azaldılmasına, eyni zamanda sistemlərin təhlükəsizliyinin təmin edilməsinə yönəlmişdir.

Ölkəmiz bir çox beynəlxalq və regional müqavilələrə üzv olmuş və kibercinayətkarlıqla mübarizədə qanunvericiliyin təkmilləşdirilməsinə daima çalışaraq buna nail olmağa səy göstərir. Kibercinayətkarlıqla mübarizədə ən çox 23 noyabr 2001-ci il tarixli Budapeşt konvensiyasının müddəalarına istinad olunur [10, s.3].

Kibercinayətkarlığa qarşı mübarizədə Azərbaycan Respublikası "MDB-nin iştirakçısı

olan dövlətlərin kompüter informasiya sahəsində cinayətlərə qarşı mübarizədə əməkdaşlığı haqqında" Sazişə də istinad edir.

Respublikamız kibercinayətkarlıqla mübarizədə həm İNTERPOL-la, həm də EUROPOL-un nəzdində olan Avropa Kibercinayət Mərkəzi ilə qarşılıqlı fəaliyyət göstərir.

Kibercinayətlərlə mübarizədə bir vasitə kimi beynəlxalq elmi konfransların, seminarların, konqres, simpozium və forumların da rolu böyükdür.

Kibercinayətkarlıqla mübarizə üzrə səlahiyyətli qurum qismində Dövlət Təhlükəsizlik Xidmətinin fəaliyyəti daim təkmilləşdirilərək yüksək texnologiyalara dair xüsusi bilik və bacarıqlara yiyələnməyi tələb edir.

Qeyd olunmalıdır ki, kibercinayətlərin istintaqının aparılması, bu istiqamətdə baş verəcək təhdidlərin önlənməsi ilə bağlı DTX tərəfindən daima müvafiq tədbirlər görülür, cinayət işləri başlanılır. Belə neqativ təzahürlərə qarşı səmərəli mübarizə aparılır [11, s.156-157].

Kibertəhlükəsizliyin təmin edilməsində Azərbaycan Respublikasının Rabitə və Yüksək Texnologiyalar Nazirliyinin uğurlu fəaliyyətini də qeyd etmək lazımdır.

Beləliklə, kibercinayətkarlıqla mübarizədə yüksək rəqəmsal texnologiyalardan istifadə olunması və ölkələrlə beynəlxalq əməkdaşlığın aparılması böyük rol oynayır. Habelə, kibertəhlükəsizlik sahəsində maarifləndirmə və preventiv tədbirlərin görülməsi kibercinayətlərin qarşısının alınmasında mühüm bir vasitədir.

Kibertəhlükəsizliklə bağlı gündən-günə artan narahatlığı nəzərə alaraq "Kibercinayətkarlıq haqqında Qanunun qəbul edilməsi məqsədəuyğundur.

Kibercinayətkarlığın tarixi ölkəmizdə yeni olsa da, lakin onun insanlara vurduğu ziyan milyon manatlarla hesablanır. Azərbaycan Respublikası CM-nin 30-cu fəslində nəzərdə tutulan 5 maddədən ibarət "Kibercinayətlər" artıq bəsit görünür. Kibercinayətkarlığa qarşı mübarizədə CM-nə daha sərt cəzalar nəzərdə tutan maddi və prosessual normaların qəbul edilməsinə artıq zəruri ehtiyac vardır [12, s.236].

Ədəbiyyat siyahısı:

1. İ.M. İsmayılov. Süni intellekt. Bakı, MAA, 2023, 233 s.
2. Kibercinayətlər haqqında Konvensiya. Budapeşt, 23 noyabr, 2001-ci il, 28 s.
3. Шур Э. Имя преступное общество. М., 1979
4. İ.M.Rəhimov. Cinayət və cəzanın fəlsəfəsi. Bakı, "Şərq-Qərb" nəş. 2024, 319 səh
5. Çezare Bekkaria. Cinayətlər və cəzalar haqqında. Bakı, "Hüquq ədəbiyyatı", 2011, 131 s.
6. Ş.M.Kərimov. Azərbaycan Respublikasında Kibercinayətkarlıq fəaliyyəti və onun səciyyəvi xüsusiyyətləri. "Hüquq elmləri və təhsil" jurnalı, Bakı 2024, №76, 62-70 s.
7. Ромашев Ю.С. Международное правоохранительное право. М. 2010. 253 с.
8. O.Məmmədov, E.Rzayev, N.Hüseynov. Daxili İşlər Orqanlarında xüsusi texnika və kibertəhlükəsizlik fəaliyyəti. "Bakı" nəş, 2023, 207 s.
9. Kibercinayətlərin istintaqına dair. Metodik vəsait. Bakı, 2022, 66 s.
10. Müstəqil Dövlətlər birliyinin iştirakçısı olan dövlətlərin kompüter informasiyası sahəsində cinayətlərə qarşı mübarizədə əməkdaşlığı haqqında" 01 iyul 2001-ci il tarixli Minsk Sazişi
11. S.T.Məcidli Kibercinayətlər. Bakı, 2019, 199 s.
12. Azərbaycan Respublikasının Cinayət Məcəlləsi. Bakı, "Hüquq Yayın Evi", 2023, 899 s.

CYBERCRIME AND ITS CRIMINAL-LEGAL FIGHT

KARIMOV SHOKHLET

Associate Professor of the Department of MAA "Law",
Doctor of Philosophy of Law

ABDURAKHMANOV SHAIR

Senior Lecturer of the Department of MAA Law

SUMMARY

The article is dedicated to cybercrime and methods of criminal-legal struggle against it. It shows that cybercrimes cause significant harm to computer systems, information technology networks, societal information security, and cyber interests. The article also indicates that people create new technologies for beneficial purposes. However, in some cases, these technologies are also used for criminal objectives.

The article extensively uses the provisions of the Budapest Convention in combating cybercrime. At the same time, the role of international cooperation in preventing cybercrime is emphasized.

Additionally, the article discusses the importance of awareness-raising and preventive measures in preventing cybersecurity threats.

SİBER SUÇ VE CEZAİ HUKUKİ MÜCADELESİ

KERIMOV ŞÖHLET

MAA "Hukuk" Bölümü Doçenti,
Hukuk Felsefesi Doktoru

ABDURAHMANOV ŞAIR

MAA "Hukuk" Bölümünün Öğretim Görevlisi

ÖZET

Makalede siber suçlar ve ceza hukuku bağlamında bununla mücadele yöntemleri ele alınmaktadır. Makalede siber suçların bilgisayar sistemlerine, bilgi teknolojilerine, kamu güvenliğine ve siber çıkarlara önemli zararlar verdiği ortaya konuyor.

İnsanların yeni teknolojileri iyilik amacıyla yarattığı ancak bazı durumlarda bu teknolojilerin suç amaçlı kullanıldığı da belirtiliyor.

Makalede ayrıca siber suçlarla mücadelede Budapeşte Sözleşmesi'nden de kapsamlı bir şekilde yararlanılıyor. Aynı zamanda siber suçların önlenmesinde uluslararası iş birliğinin önemi vurgulanıyor.

Makalede ayrıca siber tehditleri önlemeye yönelik eğitim ve önleyici faaliyetler gibi tedbirler de ele alınıyor.