Kamran XƏLİLOV
Bakı Dövlət Universitetinin Hüquq fakültəsinin
Cinayət prosesi kafedrasının doktorantı
e-mail: kamran.khalilov.isa@bsu.edu.az
ORCID ID: https://orcid.org/0000-0002-0086-009X
https://doi.org/10.6213/SANW2436

KİBERCİNAYƏTKARLIQ MÜHİTİNDƏ FİŞİNQ HÜCUMLARININ TÖRƏDİLMƏ ÜSULLARI VƏ ONUNLA MÜBARİZƏNİN HÜQUQİ ƏSASLARI

XÜLASƏ

Müasir rəqəmsal dünyada dövlət qurumlarını, cəmiyyətləri və ayrı-ayrı fərdlərin həyatını təhdid edən kibercinayətlərin sayı durmadan artmaqda davam edir. Bu kiber təhlükələrdən biri də gündəlik həyatda tez-tez qarşılaşdığımız fişinq hücumlarıdır. Kibercinayətkarlar tərəfindən ən çox müraciət edilən, həmçinin bütün internet istifadəçiləri üçün böyük təhlükə yaradan və müəyyən edilməsi çətin olan fişinq hücumları hüquq-mühafizə orqanları ilə vətəndaşların birgə əməkdaşlıq fəaliyyətini zəruri edir. İlkin mərhələdə, fişinq insanlardan məlumat oğurlamağın ən ibtidai və rahat üsullarından biri kimi görünsə də, yüksək peşəkarlıq tələb etmədiyi üçün potensial zərərvurma qabiliyyətinə malikdir və geniş çeşidli şəxsi məlumatların əldə edilməsi üçün istifadə olunur.

Bu baxımdan, fişinq hücumlarının cinayətkar xarakteristikasını bilmək və ona qarşı mümkün tədbirləri təmin etmək vacibdir. Bu məqalə kibercinayətlərin bir növü kimi fişinq hücumlarının xarakteristikasını müəyyən etməklə, onun ictimai təhlükəlilik dərəcəsini izah edir. Həmçinin bu tədqiqat vasitəsilə kibercinayətkarlıqla mübarizə çərçivəsində fişinq hücumlarına qarşı adekvat tədbirlərin görülməsi üçün müvafiq təkliflər təqdim edilir.

Açar sözlər: *fişinq, kibercinayət, hücum, təhlükə, elektron poçt.*

Fişinq sözü ingilis dilindən tərcümədə "balıq ovu" mənasını verməklə, kibertəhlükəsizlik sahəsində istifadə edilən zərərli fəaliyyət növü kimi başa düşülür. Bu cinayətkar fəaliyyət üçün belə bir ifadənin seçilməsi təsadüfi deyil. Bildiyimiz kimi, balıq ovlanması prosesi balıqların bilməyərəkdən tələyə düşməsi yolu ilə baş verir. Məhz haqqında danışdığımız kibercinayət növünün əsas icra üsulu da fırıldaqçılar tərəfindən qurbanlara təqdim edilən yalançı, saxta və feyk təkliflər, yəni insanlar üçün qurulmuş tələlərdir. Fişinq dedikdə, qanunsuz maddi və digər mənfəətlər əldə etmək üçün saxta kommunikasiya alətləri (elektron poçt, veb-saytlar və s.) vasitəsilə fərdi və ya maliyyə məlumatlarını ələ keçirmək məqsədi daşıyan cinayətkar fəaliyyət başa düşülür [29].

Fişinq hücumlarının tarixi elə də qədim deyil. Belə ki, tarixdə ilk fişinq hücumu 2004-cü ildə Kaliforniyalı bir yeniyetmənin "America Online" saytının saxta surətini yaratması ilə başladı. Bu feyk veb-sayt istifadəçilərdən məxfi məlumatları əldə edə və onların hesablarından pul çıxarmaq üçün kredit kartı məlumatlarına daxil ola bilmişdi [18, s.25].

Yaşadığımız rəqəmsal dünyada artan kiber təhdidləri nəzərə aldıqda, fişinq hücumları insanların məlumatlarını ələ keçirməyin ən vacib üsullarından biri kimi qarşımıza çıxır. Hər şeydən öncə, bu növ hücumlar qurbanların elektron poçt ünvanlarını hədəf alır. Fişinq hücumları aşkar edildiyi gündən oxşar üsullardan istifadə edilir və qurbanları tələyə salmaqda kifayət qədər "uğura" sahibdir. İlkin mərhələdə bunlar qarşı tərəfə mü-

kafatlar, hədiyyələr və s. kimi saxta mesajlar göndərməklə həyata keçirilir. Burada əsas məqsəd şəxsin kredit kartı və ya şəxsiyyəti barədə həssas məlumatları ələ keçirməkdir. Fırıldaqçılar bu məlumatdan müxtəlif məqsədlər üçün istifadə edə bilərlər. E-poçt və veb-sayt vasitəsilə həyata keçirilən fişinq fəaliyyətlərindən başqa, kibercinayətkarlar tərəfindən inkişaf etdirilən digər növ fişinq hücumları da mövcuddur. Bunlardan "vishing" (səsli fişinq), "smishing" (SMS fişinq) kimi növləri misal göstərmək olar [1, s.1235].

Fişinq hücumları kibercinayətkarların insanları manipulyasiya etmək və onların həssas məlumatlarını əldə etmək məqsədi daşıyan ən çox yayılmış sosial mühəndislik üsullarından biridir. Bu hücumların sahibləri qurbanları aldadır ki, zərərli proqramları öz texniki cihaz mənbələrinə yükləsinlər və ya etibarlı görünən e-poçt, sosial media, mətn mesajları (SMS) və ya onlayn söhbət proqramları vasitəsilə şəxsi məlumatlarını ələ keçirsinlər [6, s.1].

Hazırda istifadə edilən fişinq hücumlarının bir çox tipləri mövcud olsa da, daha çox müraciət edilən növləri aşağıdakılardır: 1) Nizə fişinqi (Spear Phishing) - bu tip hücumda kibercinayətkarlar konkret şəxsi hədəfə alır və onlara etibarlı görünən e-poçt, mətn mesajları və ya sosial media mesajları göndərirlər. Onlar tez-tez həssas məlumat əldə etmək məqsədi ilə qurbanın həmkarı və ya tanışı kimi davranırlar:

[Nümunə]:

"Mövzu: İllik bonuslar haqqında vacib məlumat!

Məzmun: Hörmətli,..... X şirkətinin İnsan Resursları şöbəsinin rəsmi nümayəndəsi olaraq Sizə yazıram. Şirkətimizin yeni bonus siyasəti ilə tanış olmaq üçün aşağıdakı faylı yükləyin. Ən son xəbərlərdən məlumatlı olmaq üçün ən rahat yol: [troyan fay]" [31].

2) Balina ovu (Whaling) - əsasən korporativ rəhbərlər, sahibkarlar və ya ciddi media rəhbərləri kimi yüksək reputasiyaya sahib şəxsləri hədəf alan üsuldur. Belə hücumlarda dövlət qurumları və ya mühüm təşkilatlar adından göndərilmiş kimi görünən saxta e-poçtlar ilə qurbanın məlumatını əldə etməyə cəhd edilir:

[Nümunə]:

"Mövzu: Xidməti müqavilənin təsdiqlənməsi barədə

Məzmun: "Hörmətli..., Şirkətimiz ilə Sizin müəssisəniz arasında imzalanacaq yeni xidməti müqavilənin ilkin versiyası hazırdır. Bununla bağlı olaraq, qoşmada əlavə olunmuş sənədi nəzərdən keçirməyinizi və uyğun olduğu təqdirdə təsdiqləməyinizi xahiş edirik. Sənədə keçid üçün aşağıdakı linkdən istifadə edin: (saxta link)." [32].

3) Səsli fişinq (Vishing) – Bu yolla cinayətkar dövlət qurumlarının, bankların və ya hüquq- mühafizə orqanlarının nümayəndəsi olduqlarını iddia edərək telefon vasitəsilə qurbanlarını aldatmağa çalışırlar. Onlar tez-tez təhdid və ya inandırıcı dildən istifadə edərək şəxsi məlumatların paylaşılmasını təmin etməyə cəhd edirlər. Bu zaman əsas vasitə kimi fırıldaqçılar qarşıdakı şəxsin məlumatlarının məhv olma və ya oğurlanma təhlükəsi altında olduğunu deyərək təzyiq etməyə çalışırlar:

[Nümunə]:

"Telefon zəngi:

Salam, Sizi ..... Bankdan narahat edirik. Mən, A.Babayev, Bankın təhlükəsizlik şöbəsinin əməkdaşıyam. Sizin hesabınızda şübhəli əməliyyat aşkarladıq. Sizin adınızdan 200 manat məbləğində ödəniş təsdiqlənməyə çalışılıb. Əgər bu əməliyyat Sizin tərəfinizdən edilməyibsə, hesabınızı dərhal bloklamağınız lazımdır. Bunun üçün zəhmət olmasa kartınızın 16 rəqəmli nömrəsini və Sizə göndərəcəyimiz SMS vasitəsilə gələn təsdiq kodunu deyin." [23, s.4,5].

4) SMS fişinqi (Smishing) – bu növdə fırıldaqçılar öz qurbanlarına özlərini tanış şəxs, bank və ya xidmət təminatçısı kimi təqdim edərək SMS mesajları göndərirlər. Qurbanlardan ödəniş etmələri və ya şəxsi məlumatlarını paylaşmaları xahiş olunur. Onlar həmçinin Vatsap və Feysbuk kimi platformalardan doğrulama kodları tələb edərək istifadəçi hesablarını oğurlamağa çalışırlar:

[Nümunə]:

"SMS mətni:

Hörmətli müştəri! Hesabınızda təhlükəsizlik problemi aşkarlanmışdır. Xahiş edirik, dərhal hesabınızı təsdiqləmək üçün aşağıdakı linkə keçid edin: [saxta link]. Əks halda hesabınız bloklana

bilər." [20, s.546; 15, s.56-58].

5) Ferma fişinq (Pharming) - veb-sayt trafikinin manipulyasiya edildiyi və məxfi məlumatların oğurlandığı fişinqə bənzər kibercinayətkarlığın bir növüdür. Bağlantı yaratmaq üçün www.google.com kimi internet ünvanını təşkil edən hərflərin ardıcıllığı DNS serveri tərəfindən IP ünvanına (Internet Protocol address) çevrilməlidir. Belə ki, DNS sözü "Domain Name System" sözlərinin qısaltmasıdır və internetdəki kompüterlərin, cihazların və ya resursların IP ünvanlarını daha mənalı və yaddaqalan domen adlarına birləşdirən sistemdir. IP ünvanları ədədi formada olduğundan insanlar tərəfindən asanlıqla yadda qalmaya bilər. DNS bu ədədi IP ünvanlarını insanların daha asan başa düşə biləcəyi domen adlarına çevirir. Məsələn, veb-brauzerə www.youtube.com yazdığımız zaman DNS bu domen adını müvafiq IP ünvanına çevirir və sorğunun düzgün serverə çatmasını təmin edir [16, s.36].

Bu kibercinayət üçün əsasən iki hücum üsulu mövcuddur: Birincisi, şəbəkə trafikini orijinal hədəfdən uzaq bir xakerin kompüterinə yönləndirməkdir. Bu zaman istifadəçini saxta veb-sayta göndərmək üçün kompüterin host fayllarını dəyişdirən virus və ya troyan yüklənir. İkincisi, xaker DNS serverini dəyişdirərək, birdən çox istifadəçinin bilmədən saxta sayta daxil olmasına səbəb olur. Saxta veb-sayt istifadəçinin kompüterinə viruslar və ya troyanlar quraşdırmaq üçün istifadə olunur. "Sayt trafikinin yenidən istiqamətləndirilməsi" kibercinayətin xüsusilə əlaqəli formasıdır. Çünki DNS server dəyişdirilərsə, təsirə məruz qalan istifadəçi zərərli proqramlardan tamamilə təmizlənmiş kompüteri olsa belə, qurbana çevrilə bilər. Veb-sayt ünvanını əl ilə daxil etmək və ya həmişə etibarlı əlfəcinlərdən istifadə etmək kimi ehtiyat tədbirlərin görülməsi kifayət deyil [16, s.38]. Bu cür saxtakarlıqlardan qorunmaq, şübhəli veb-saytlara daxil olmaq və ya şübhəli e-poçt mesajlarındakı bağlantıları kliklәməmək lazımdır. Digər müdafiə üsulu kimi, sistem hesablama proqramları ilə istifadə olunan etibarlı "anti-malware" və "anti-virus" həllini quraşdırmaqla da qoruna bilər. Bu addımlar zərərli proqramların əksəriyyətinin kompüterə daxil olmasının və host fayllarının dəyişdirilməsinin qarşısını alır.

1. Ferma fişinqi ümumilikdə adi fişinq hücumu kimi görünsə də, əslində icra olunma üsullarına, xarakterinə və təhlükəlilik dərəcəsinə görə bir-birindən fərqlənir. Bu fərqi aşağıdakı cədvəldə daha aydın görmək olar:

Cədvəl 1. Ferma fişinqi (Pharming) və adi fişinq arasında müqayisə cədvəli [22, 30]:

Meyar	Adi fişinq	Ferma fişinqi
Hücumun icra üsulu	E-poçtlar, SMS-lər və sosial media vasitəsilə göndərilən linklər vasitəsilə	DNS manipulyasiyası və ya zərərli proqamlar vasitəsilə
Qurbanın iştirakı	İstifadəçi tərəfindən zərərli linkə keçid etməklə baş verir	İstifadəçi heç bir əlavə prosedur etmədən saxta sayta yönləndirilir
Təhlükənin dərəcəsi	Əsasən fərdi istifadəçiləri hədəf alır	Kütləvi şəkildə bir çox istifadəçini eyni anda hədəf ala bilər
Əks tədbirlər	E-poçtlara və mesajlara diqqət yetirmək, filtrasiya xidmətindən istifadə etmək, rəsmi URL-ləri yoxlamaq vacibdir	DNS təhlükəsizlik mexanizmlərindən və ya etibarlı DNS serverlərdən istifadə etmək vacibdir

Aparılmış müqayisələrdən və nümunələrdən də göründüyü kimi, fişinq hücumları əksər hallarda elektron poçtlar vasitəsilə həyata keçirilir. Bu baxımdan, fişinq hücumlarının qurbanı olmamaq üçün bu tip mesajların hansı xüsusiyyətlər daşıdığını konkret nümunə ilə analiz etməkdə fayda vardır. Belə ki, saxta e-poçtu müəyyən etməyin iki yolu vardır: Birincisi odur ki, əgər mesajın mövzu hissəsində aşağıda göstərilən tipdə cümlələrdən istifadə edilirsə, fişinq ehtimalı yüksəkdir. Məsələn, 1) abc@example.com e-poçt hesabınız sındırılıb; 2) Təcili: E-poçt hesabınızın parolunu dərhal dəyişin; 3) Bank hesabınıza müdaxilə edilib; 4) Təhlükəsizlik Xəbərdarlığı: E-poçt hesab-

larınızı qeydiyyatdan keçirin və s. İkincisi, əgər göndərilmiş e-poçtda istifadəçidən hansısa tələblərin yerinə yetirilməsi tələb olunursa, deməli fişinq hücumu potensial həddədir. Məsələn; 1) Şəxsi məlumatlarınız və ya bank hesabı məlumatlarınız; 2) Müəyyən hesaba pul göndərilməsini xahiş etmək; 3) Parolun dəyişdirilməsini tələb etmədiyiniz halda parol sıfırlama linki almaq; 4) Detalları yoxlamaq üçün digər naməlum bağlantılara yönləndirilmək və s. [2].

Fişinq hücumlarını həyata keçirərkən kibercinayətkarlar fərqli, amma bir-birilə yaxından əlaqəli psixoloji manevrlər tətbiq edirlər. Belə ki, kibercinayətkarlar fərdlərin qərar qəbul etmə proseslərinə təsir göstərmək üçün güclü emosiyalara müraciət edərək, onları müəyyən hərəkətlər etməyə məcbur edir. Məsələn, həvəsləndirmə, vaciblik, qorxu kimi insani hisslər istismar olunur. Buna uyğun olaraq, linkə klikləmək, əlavə yükləmək və ya formanı doldurmaq müqabilində qurbanlara maliyyə mükafatı və ya xüsusi sövdələşmə təklif olunur. Bəzən cinayətkarlar vaxt baxımından təzyiq yaratmaq və sürətli hərəkətə keçmək üçün fövqəladə ssenarilər yaradırlar. Həmçinin qurbanlar müəyyən profilaktiki tədbir görməsələr bank hesabının dayandırılması və ya digər uydurma "qanuni hərəkətlərlə" hədələnirlər [19, s.5].

Bir çox kibercinayətlər kimi fişinq də özlüyündə bir neçə mərhələdə həyata keçirilir. Nəzəriyyədə müxtəlif yanaşmalar olsa da, şərti olaraq 3 əsas mərhələdən ibarətdir:

I mərhələ - Məlumat toplanılması və plan hazırlanması: Bu mərhələdə fişerlər qurbanlarını, əldə ediləcək məlumatları və hücumda hansı texnikadan istifadə edəcəklərini müəyyən etməklə hücumlarını planlaşdırmağa başlayırlar. Fişçilərin hədəflərini seçmək üçün düşündükləri əsas cəhət ən aşağı xərclə və mümkün olan ən az risklə maksimum qazancı necə əldə etməkdir. Daha dəqiq desək, kibercinayətkarlar potensial qurbanların davranışları, maraqları və zəiflikləri barədə sosial media platformaları, açıq mənbə kəşfiyyatı (OSINT) və digər vasitələrlə məlumat əldə etməyə çalışırlar. Daha sonra, toplanmış etibarlı informasiya əsasında təcavüzkarlar saxta e-poçtlar, veb-saytlar və ya digər kommunikasiya vasitələri hazırlayırlar. Bu tələlər real təşkilatların və ya şəxslərin fəaliyyət tərzinə və ya istəklərinə bənzədilir ki, qurbanı aldatmaq daha rahat olsun. Məsələn, belə hücumlar zamanı "Google", "Microsoft", "Apple", "Chrome" kimi məşhur şirkətlərin rəsmi e-poçt mesajları təqlid oluna bilər.

II mərhələ - Hücuma keçilməsi və təqdim etmə: Bu mərhələdə artıq hazırlanmış tələlər istifadəçilərin diqqətinə çatdırılır. E-poçtlar, sms-lər, sosial media mesajları və ya səsli zənglər vasitəsilə həyata keçirilən bu hücumlar qurbanları zərərli linklərə daxil olmağa təşviq edir. Bundan sonra, qurban tələyə düşərsə, həm məlumatlarını itirə, həm də sistemi zərərli proqram təminatları (məsələn, "ransomware") və ya viruslarla yoluxdura bilər.

III mərhələ - Məlumatların ələ keçirilməsi və istifadəsi: Sonuncu mərhələdə fırıldaqçılar əldə etdikləri məlumatları müxtəlif üsullarla istifadə edə bilərlər. Buraya birbaşa maliyyə fırıldaqları, identifikasiya oğurluğu, şantaj kimi qurbanın şərəf və ləyaqətinə xələl gətirəcək qanunsuz fəaliyyətlər daxildir. Həmçinin əldə edilmiş məlumatlar qara bazarda satışa çıxarıla bilər [17, s.1112].

Fişinq 21-ci əsrin ən mütəşəkkil cinayətlərindən biridir. Bu, zərərli proqram növü və ya kiminsə təsadüfi qurbanlara onlar haqqında şəxsi məlumat almağa çalışmaq üçün saxta e-poçt göndərdiyi termin kimi müəyyən edilir. Daha dəqiq desək, hesablama sahəsində fişinq sosial mühəndislik üsullarından istifadə edərək veb-saytın saxta versiyalarını elektron poçtla göndərməklə məşhur veb-saytların istifadəçilərini aldatmağa cəhd edir. Bunun qarşısını almaq asan görünə bilər, lakin fişinq hücumlarında baş verən texnoloji innovasiyalar, kibercinayətkarların yeni üsullar axtarışı bu növ cinayətlərin müəyyən edilməsində bəzi çətinliklər yarada bilər [12, s.15].

Beləliklə, fişinq hücumları kibercinayətkarların fəaliyyətində ən çox müraciət edilən sahələrdən biridir və istər maliyyə təsiri baxımdan, istərsə də texniki təhlükəsizlik baxımından hazırda kifayət qədər mənfi reytinqə sahibdir. Fişinq hücumları üzrə statistik göstəricilər də bunu sübut edir. Bununla əlaqədar aşağıdakı cədvələ diqqət yetirməkdə fayda vardır:

Cədvəl 2. Fişinq hücumları üzrə statistik göstəricilər [25,26,27,28]:

Parametr	Statistik göstərici	Məlumatı təmin edən mənbələr
Qlobal kiberhücumlarda "fişinq"in payı	91%	Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti
Fişinq hücumlarının qlobal iqtisadiyyata təsiri	10.5 trilyon ABŞ dolları	Global Cybersecurity Outlook 2025
Fidyə xarakterli fişinq hücumlarında cinayətkarların gəliri	814 milyon ABŞ dolları	Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti
Fişinq hücumlarında ən çox istifadə edilən şirkətlər	"Microsoft" – 32% "LinkedIn" – 11% "Apple" – 12% "WhatsApp"- 3% "Google" – 12% "Facebook" – 2%	"Azərtac" İnformasiya Agentliyi
İstifadəçilərin fişinq hücumları ilə qarşılaşma ehtimalı	90%	Global Cybersecurity Outlook 2025
Süni intellekt vasitəsilə edilən fişinq hücumlarının payı	4,7%	Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti

Göründüyü kimi, fişinq hücumları kibertəhlükəsizlik sahəsində kifayət qədər təsirə malikdir. Bunun səbəbləri müxtəlifdir və onları bir neçə qrupda birləşdirmək mümkündür: 1) internet istifadəçilərinə münasibətdə yetərli səviyyədə maarifləndirmə işlərinin aparılmaması; 2) göndərilən mesajlarda insanları həvəsləndirmək üçün müxtəlif maliyyə riçarqlarından və pul tələsindən istifadə edilməsi; 3) bir çox e-poçt təhlükəsizlik sistemlərinin fişinq mesajlarını spam mesajı kimi nəzərə ala bilməməsi; 4) geniş yayılmış IoT (İnternetin əşyaları) cihazları və bu cihazlarla toplanan məlumatların nəzarətsiz şəkildə və təhlükəsizlik tədbirləri xaricində saxlanılması və s. [5].

Fişinq hücumları ilə mübarizə hüquq-mühafizə orqanlarının qarşısında duran ən vacib məsələlərdən biridir. Lakin bu vəzifə təkcə dövlətin səlahiyyətli orqanlarının üzərinə düşmür, çünki fişinq hücumları internet istifadəçilərini gündəlik narahat edən fenomendir. Bu cür hücumlarla mübarizə təkcə milli səviyyədə deyil, həm də regional və beynəlxalq müstəvidə aparılmalıdır. Fişinq hücumları ilə mübarizənin beynəlxalq hüquqi təsbiti 2001-ci il tarixli "Kibercinayətkarlıq haqqında" Budapeşt Konvensiyasının 7-ci və 8-ci maddələrində nəzərdə tutulmuşdur. Belə ki, sözügedən normaların məzmunundan aydın olur ki, Konvensiyanı imzalayan dövlətlər kompüter texnologiyalarından istifadə etməklə məlumatların saxtalaşdırılması hallarını cinayət əməli kimi tanımaq üçün aidiyyəti hüquqi aktlar qəbul etməlidir. Burada məqsəd verilənlərin həqiqi informasiya kimi təqdim edilməsi, həmçinin məlumatların dəyişdirilməsi, silinməsi və onlara əlavələr edilməsi, eləcə də onlardan hüquqi nəticələrə səbəb olacaq fəaliyyətlərdə istifadə edilməsini diqqətə çatdırmaqdır. Sözügedən əməllərin sırasına kompüter məlumatlarının qanunsuz daxil edilməsi, dəyişdirilməsi və bloklanması; kompüter sisteminin fəaliyyətinə müdaxilə etməklə digər şəxsin əmlakına ziyan vurulması və ya onu əmlakdan məhrum etmə halları daxildir [14].

Qeyd edilməlidir ki, bir sıra inkişaf etmiş ölkələrin qanunvericilik sistemlərində fişinq hücumları artıq müstəqil cinayət tərkibi kimi tanınmış və ayrıca maddələrlə tənzimlənmişdir. Məsələn, Almaniya Cinayət Məcəlləsinin (Strafgesetzbuch – StGB) 202b maddəsi "fişinq" adlanır və kimsə tərəfindən texniki vasitələrlə, özünə və ya başqasına aid olmayan, qeyri-ictimai məlumat emalı qurğusundan və ya belə bir qurğunun elektromaqnit yayımından, ona aid olmayan mə-

lumatları qanunsuz olaraq ələ keçirməsi" şəklində xarakterizə olunur və müvafiq əməlin törədilməsi iki ilə qədər azadlıqdan məhrumetmə cəzası və ya cərimə ilə cəzalandırılır. Həmçinin 202c maddəsinin dispozisiyasına əsasən parolların və ya digər təhlükəsizlik kodlarının hazırlanması, əldə edilməsi, satılması və ya yayılması, eləcə də fişinq hücumları üçün proqram təminatlarının hazırlanması və ya yayılması əməllərinin törədilməsi "Məlumat casusluğuna və fişinqə hazırlıq fəaliyyətləri" adlanır və ayrıca maddə kimi öz təsbitini tapmışdır [11].

Estoniya Cinayət Məcəlləsində (Karistusseadustik) isə fişinq cinayətləri, xüsusilə 213-cü (Kompüterlə bağlı fırıldaqçılıq) və 217-ci (Kompüter sistemlərinə qanunsuz girişin əldə edilməsi) maddələrində mülkiyyət mənfəəti məqsədilə kompüter proqramlarına və ya məlumatlara qanunsuz daxil olmaq, dəyişdirmək, silmək, zədələmək və ya bloklamaq yolu ilə başqa şəxsə əmlak ziyanının vurulması, eləcə də elektron məlumatların saxtalaşdırılması və icazəsiz əldə edilməsi kontekstində xüsusi tənzimləmə predmetinə çevrilmişdir. Estoniya bu sahədə qabaqcıl ölkələrdən biri hesab olunur və onun qanunvericiliyi Avropa İttifaqı direktivlərinə uyğunlaşdırılmışdır [13]. Həmçinin 2024-cü ildə keçirilən "PhishOFF" adlı beynəlxalq polis əməliyyatı nəticəsində fişinq hücumları üçün istifadə edilən "LabHost" platformasının ləğv edilməsində Estoniya mühüm rol oynamışdır. Burada fişinq əməli texniki və sosial mühəndislik üsullarının sintezindən ortaya çıxan kompleks cinayət kimi qiymətləndirilir.

Avropa İttifaqının 2013/40/EU saylı direktivi də fişinq hücumlarını kompüter sistemlərinə qarşı cinayətlər kontekstində qiymətləndirir və üzv dövlətlərə bu cinayətlər üçün konkret cinayət tərkiblərinin yaradılmasını tövsiyə edir. Həmin direktivin 3-cü maddəsində "icazəsiz giriş", 4-cü maddəsində isə "icazəsiz məlumat əldə etmə və saxtalaşdırma" hallarına yer verilmişdir ki, fişinq bu kateqoriyalara uyğun gəlir [8]. Bundan başqa, 2019/713/EU saylı direktiv nağdsız ödəniş vasitələrinin dələduzluğu və saxtalaşdırılması ilə mübarizə aparmaq məqsədilə qəbul edilmişdir. Fişinq hücumları nəticəsində əldə olunan ödəniş məlumatlarının istifadəsi bu direktiv çərçivəsində cinayət hesab olunur [9].

Bu təcrübələr göstərir ki, beynəlxalq hüquq sistemləri fişinq hücumlarını yalnız klassik informasiya cinayətləri çərçivəsində deyil, yeni nəsil kibercinayətlər kontekstində nəzərdən keçirir və onları ayrıca hüquqi kateqoriya kimi formalaşdırmaqla mübarizənin effektivliyini artırmağa çalışırlar. Azərbaycan Respublikası üçün də bu yanaşmanın tətbiqi fişinq hücumlarının hüquqi təsnifatının dəqiqləşdirilməsi və hüquqi mexanizmlərin gücləndirilməsi baxımından zəruridir.

Hazırda Azərbaycan Respublikasının Cinayət Məcəlləsində fişinq hücumları vasitəsilə şəxsi və maliyyə məlumatlarının əldə olunması və bu cinayətkar fəaliyyətə bağlı olaraq həyata keçirilən oxşar qanunsuz əməllərin kriminallaşdırılması ayrıca maddə kimi nəzərdə tutulmasa da, ilkin olaraq, Məcəllənin 272-ci (Kompüter məlumatlarını qanunsuz ələ keçirmə) və 273-cü (Kompüter sisteminə və ya kompüter məlumatlarına qanunsuz müdaxilə) maddələri fişinq xarakterli hücumların və cinayətkar fəaliyyətlərin kriminallaşdırılmasını dolayı olaraq təmin edir. Belə ki, müvafiq normalarda kompüter məlumatlarının qanunsuz ələ keçirilməsi və yayılması, eləcə də məlumatlarda bu və digər şəkildə dəyişikliklərə səbəb ola biləcək hərəkətlərin edilməsi bu növ hücumların realizəsi qismində başa düşülə bilər. Həmçinin Məcəllənin 178-ci maddəsi (dələduzluq) üzrə dələduzluq hərəkətlərinin rəqəmsal şəraitdə icrası bu tip hücumların realizəsi kimi başa düşülə bilər [3]. Lakin Azərbaycan Respublikasının cinayət qanunvericiliyində konkret olaraq fişinq hücumları ilə icra olunan cinayətkar əməllər ayrıca olaraq göstərilməmişdir. Bu baxımdan, qeyd olunan maddələr cinayətkarın məqsədini, hücumun texniki mexanizmini və əməlin ictimai təhlükəlilik dərəcəsini tam şəkildə ehtiva etmir. Buna görə də, fişinq hücumlarının konkret cinayətkar əməl kimi ayrıca bənd (və ya yarımbənd) şəklində AR CM-də kriminallaşdırılması zəruri addım hesab edilə bilər.

Fikrimizcə, bu zərurət özünü bir neçə formada göstərir. Birincisi, fişinq hücumlarının məq-

sədi şəxslərin fərdi məlumatlarını, bank kartı və hesab rekvizitlərini, identifikasiya vasitələrini aldatma yolu ilə ələ keçirməklə, həmin məlumatlar üzərindən qeyri-qanuni maddi gəlir və ya digər fayda əldə etməkdir. Bu əməldə klassik dələduzluq ilə oxşarlıqlar olsa da, fişinq cinayətlərində kiberməkanın imkanlarından sui-istifadə və texniki manipulyasiya ilə sosial mühəndisliyin sintezi xüsusi element kimi çıxış edir. Məhz bu özəllik onu müstəqil cinayət tərkibi kimi nəzərdən keçirməyi aktuallaşdırır. İkincisi, fişinq hücumları çox vaxt xarici ölkə mənşəli serverlər və saxta platformalar vasitəsilə həyata keçirilir. Hücum edənlərin şəxsiyyəti gizli qalmaqla yanaşı, bu cinayətlər çox zaman beynəlxalq qruplaşmalar tərəfindən təşkilatlanmış şəkildə icra edilir. Bu baxımdan fişinq cinayətləri transmilli cinayət əlamətləri daşıyır və BMT-nin 2000-ci il tarixli "Transmilli Mütəşəkkil Cinayətkarlığa qarşı Palermo Konvensiyası"nın 2-ci maddəsində təsbit olunan transmilli cinayət tərifinə uyğun gəlir [24]. Belə ki, hücumların texniki icrası ilə sosial mühəndislik elementləri çox zaman ayrı-ayrı ölkələrdə yerinə yetirilir, hədəfə alınan fərdi və ya maliyyə məlumatları transmilli cinayətkar şəbəkələr tərəfindən oğurlanaraq digər ölkələrdə istifadə edilir və nəticədə cinayətin təsiri coğrafi sərhədləri aşır. Məsələn, Azərbaycanda yerləşən serverə və ya istifadəçiyə Nigeriyada yerləşən şəxslər tərəfindən fişinq e-poçtları göndərilə və nəticədə əldə edilmiş bank məlumatları üçüncü bir ölkədə nağdlaşdırıla bilər. Bu isə fişinq cinayətlərini təkcə "internet fırıldaqçılığı" kimi deyil, həm də transmilli mütəşəkkil cinayətkarlığın bir forması kimi dəyərləndirməyə əsas verir. Azərbaycan Respublikası 13 may 2003-cü il tarixli 435-IIQ nömrəli Qanunu ilə bu Konvensiyanı ratifikasiya etdiyi üçün bu tip cinayətlərlə mübarizə istiqamətində daxili cinayət hüququnun təkmilləşdirilməsi beynəlxalq öhdəliklərin icrası baxımından da vacibdir. Üçüncüsü, fişinq hücumlarının bank sektoru, dövlət elektron xidmətləri, təhsil və səhiyyə sistemləri kimi ictimai əhəmiyyətli informasiya resurslarına qarşı yönəldilməsi onların ictimai təhlükəlilik səviyyəsini əhəmiyyətli dərəcədə artırır. Bu, zərərçəkənlərin yalnız maddi itkilərinə deyil, eyni zamanda ictimai infrastrukturun funksionallığına və informasiya təhlükəsizliyinə zərbə vurur. Bu kimi əməllər hal-hazırda Cinayət Məcəlləsinin müxtəlif maddələri ilə (CM-nin 177.1, 272-273-cü maddələri) qismən əhatə olunsa da, fişinqin spesifik hüquqi və texniki xüsusiyyətlərini nəzərə alaraq, onun yalnız ümumi dələduzluq və ya informasiya sistemlərinə qanunsuz müdaxilə kontekstində deyil, həm də transsərhəd kibercinayətkarlıq çərçivəsində beynəlxalq hüququn müddəalarına əsaslanaraq ayrıca normativ tənzimləməyə ehtiyacı olduğu qənaətindəyik.

Göstərilən hüquqi və praktiki əsaslara istinadən, fişinq hücumlarının Azərbaycan Respublikası Cinayət Məcəlləsində müstəqil cinayət tərkibi kimi nəzərdə tutulması bu əmələ qarşı effektiv mübarizə və preventiv hüquqi mexanizmlərin formalaşdırılması baxımından vacibdir. Belə bir yanaşma həm fişinqin texniki və sosial xüsusiyyətlərini daha dəqiq əks etdirəcək, həm də transmilli xarakterli bu cinayət növü ilə mübarizədə beynəlxalq hüquqi əməkdaşlığa uyğun milli hüquqi çərçivə yaradacaqdır. Bu baxımdan, beynəlxalq təcrübədən çıxış edərək, fişinq hücumlarının aldatma yolu ilə fərdi məlumatların ələ keçirilməsi, elektron identifikasiya vasitələrinin qanunsuz istifadəsi və texniki manipulyasiya vasitəsilə məlumat əldə etmə kimi alt tərkiblərlə ayrıca maddə şəklində kriminallaşdırılması məqsədəuyğun hesab edilir.

Bundan əlavə, fişinq hücumlarının araşdırılmasında cinayət-prosessual aspekt də vacib məqamlardan biridir. Belə ki, bu tip hücumlar üzrə müvafiq cinayət işinin açılması, ilkin sübutların əldə edilməsi və rəqəmsal sübutların qanuniliyinin əsaslandırılması zəruri addımlardır. Bəs problem necə formalaşır? Məlum olduğu kimi, ciddi xarakterli fişinq hücumlarına məruz qalmış bir çox istifadəçi və ya təşkilatlar bu barədə hüquq-mühafizə orqanına lazımi vaxtda məlumat vermirlər. Bunun əsas səbəbi hüquqi şəxslərin reputasiya və kommersiya itkisi ilə üz-üzə qalma qorxusudur. Həmçinin bəzən fırıldaqçılarla danışıqların aparılması və bu yolla məlumatların bərpa edilməsinə olan ümid istintaq orqanlarının iş üzrə vaxtında informasiya əldə etmək imkanını məhdudlaşdırır. Nəticədə isə müvafiq kiberci-

nayət üzrə cinayət işinin başlanması ləngiyə bilir. Çünki cinayət işinin başlanması üçün kifayət qədər səbəb və əsasların olması vacibdir [4]. Lakin müvafiq kibercinayətə dair ilkin sübutların əksəriyyəti texniki və xarici platformalarda yerləşdiyi üçün cinayət işinin başlanması üçün əsasların mövcudluğu sual altına düşür. Bu problemin həlli üçün təklif edirik ki, rəqəmsal mühitlərdə baş vermiş dəyişikliklər aktlaşdırılmalı, şifrələnmiş fayl nümunələrinin və təhdid, təhrik və saxta həvəsləndirmə xarakterli mesajlar protokollaşdırılmalı və vaxtında hüquq-mühafizə orqanlarına məlumat verilməlidir.

Cinayət-prosessual baxımdan diqqət olunması digər məsələ rəqəmsal sübutların əldə edilməsi ilə bağlıdır. AR CPM-nin 135.1-ci maddəsinə əsasən *"Cinayət təqibi üzrə əhəmiyyət kəsb edə bilən məlumatları hərf, rəqəm, qrafika və digər işarə formasında özündə əks etdirən kağız, elektron və ya digər daşıyıcılar sənəd hesab olunur."* [4]. Belə ki, fişinq hücumlarından dərhal sonra və ya həmin müddətdə əldə edilən məlumatlar sonda məhkəmədə sübut kimi tanınmalıdır. Lakin problem budur ki, fişinq hücumlarında həmin sübutların orijinallığı, dataların dəyişdirilmədiyi və hüquqazidd müdaxiləyə məruz qalmadığı kimi cəhətlər sübuta yetirilməlidir. Buna görə də, sübutların toplanılması zamanı "chain of custody" (sübutların ardıcıllıqla qorunması zənciri) prinsipi tətbiq edilməli və rəqəmsal sübutlar kriptoloji üsullarla (məsələn, hash metodu) təsdiqlənməlidir.

Bundan başqa, fişinq hücumlarının ibtidai istintaqı zamanı süni intellekt əsaslı sistemlərdən istifadə edilməsi də hüquq-mühafizə orqanlarının fəaliyyətini əhəmiyyətli dərəcədə səmərəli edəcəkdir. Belə ki, avtomatik sübut axtarışı və təsnifatını həyata keçirən süni intellekt əsaslı alqoritmlər vasitəsilə - "IBM i2 Analyst's Notebook" və ya "Palantir" - minlərlə e-poçt, mesaj və IP adresləri arasında şübhəli nümunələrin aşkarlanması və sübut kimi seçilməsi təmin edilə bilər. Qeyd olunan tətbiqlər e-poçt mesajlarındakı URL (Uniform Resource Locator – hər hansı resursun ünvanı) mənbələrini avtomatik araşdırır, onların saxta olub-olmadığını mövcud məlumat bazaları ilə müqayisə edir, həmçinin qurbanla əlaqə qurulan vaxtı və üsulu analiz edərək cinayətkarın istifadə etidyi alətləri üzə çıxarır [7, s.3]. Bununla yanaşı, "Microsoft Defender SmartScreen", "Google Safe Browsing" kimi tətbiqlər süni intellektə əsaslanan domen təhlili alqorimtləri vasitəsilə intenterdə fişinq məqsədilə yaradılmış saxta saytları real vaxtda izləyir və təhlükə barədə istifadəçilərə və hüquq-mühafizə orqanlarına siqnal göndirir [10, s.8]. Həmçinin "DarkTracer" və "Recorded Future" kimi sistemlər süni intellekt tətbiqi ilə kibercinayətkarların davranış modelini öyrənərək onların keçmiş hücumlarına və istifadə etdikləri metodlara dair profil tərtib edir. Məsələn, eyni IP aralığından eyni tipli e-poçtlarla ardıcıl fişinq cəhdləri müəyyənləşdirilərsə, süni intellekt həmin istifadəçənin əvvəlki fişinq və ya ransomware hadisələrində iştirak etdiyini ehtimal edə və "modus operandi" əsasında proqnozlaşdıra bilər. Bu model vasitəsilə şübhəli və ya təqsirləndirilən şəxsin niyyəti və qanunsuz peşəkar fəaliyyəti sübuta yetirilə bilər [21, s.1112].

Nəticə olaraq, fişinq hücumları ilə hüquqi müstəvidə mübarizə aparılması hüquqi və texniki maarifləndirmənin qarşılıqlı əlaqəsi kimi nəzərə çarpan çoxşaxəli və kompleks fəaliyyətdir. Fişinq hücumlarından qorunmaq üçün maarifləndirmə işlərinin aparılması və istifadəçilərdə bu tip qanunsuz fəaliyyətlərə qarşı hüquqi sayıqlıq formalaşdırmaq vacibdir. Məhz bu kontekstdə, təhlükəsizliyi təmin etmək üçün etibarlı mənbələrə aid olmayan linklərə kliklәməkdən çəkinmək, cihazın və sistemin təhlükəsizliyini qorumaq üçün yenilənmiş və güclü təhlükəsizlik proqramından istifadə etmək çox vacibdir. Zərərli proqram və viruslara qarşı effektiv müdafiəni təmin etmək üçün təhlükəsizlik proqramlarının ən müasir versiyalarına üstünlük verilməlidir. Tətbiqlər və ya proqram təminatı şübhəli veb-saytlardan, xüsusən pulsuz yükləmələr təklif edən saytlardan əldə olunmamalıdır, çünki belə fayllarda əksərən zərərli proqramlar və ya gizlədilmiş virus mənbələri ola bilər. Əlavə olaraq, e-poçt təhlükəsizliyi üçün autentifikasiya və filtrləmə mexanizmlərindən istifadə edilməlidir. Şəxslər daim diqqətli olmalı və saxta üsullar və təhlükəsizlik təhdidlərindən xəbərdar olmağa ça-

lışmalıdırlar. Fişinq hücumlarına qarşı effektiv müdafiə strategiyalarına bu cür hücumların qarşısının alınması, onların vaxtında aşkar edilməsi və müvafiq maraqlı tərəflər arasında məlumatlılığın artırılması aiddir.

Fişinq hücumları peşəkar texniki bilik və bacarıq tələb etməsə də, müasir rəqəmsal mühitdə tez-tez istifadə olunan kibercinayət növü kimi qarşımıza çıxır. Asan və rahat üsullarla törədilməsi bu növ hücumların diqqətdən kənarda qalmasına şərait yaratmamalıdır. Potensial kiber təhlükələrdən qorunmaq üçün mütəmadi maarifləndirmə işləri aparılmalı, internet istifadəçilərinin hüquq-mühafizə orqanları ilə qarşılıqlı əlaqədə fəaliyyət göstərməsi zərurəti başa düşülməli və fırıldaqçıların oyunlarına qarşı hər zaman ayıq-sayıq hərəkət etməyi bacarmaq lazımdır.

İstifadə edilmiş ədəbiyyat:

1. Aaliyah E. Chichwadia, Noluntu Mpekoa. Detecting Smishing and Vishing Attacks using Machine Learning. International Journal of Intelligent Computing Research (IJICR), Volume 15, Issue 1, -2024. -p. 1234-1241.
2. Ahmed Aleroud, Lına Zhou. Phishing Environments, Techniques, and Countermeasures: A Survey. Computers & Security. Volume 68, (2017). -p.160-196.
3. Azərbaycan Respublikasının Cinayət Məcəlləsi. (2000). https://e-qanun.az/framework/46947
4. Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsi. (2000). https://frameworks.e-qanun.az/0/c_c_14.html
5. Bhardwaj, A., Sapra, V., *et.al.*, Why is phishing still successful? Computer Fraud & Security, 9, (2020). -p.15-19.
6. Bryon Miller, et.al., Preventıon of Phıshıng Attacks: A Three-Pıllared Approach. Issues in Information Systems. Volume 21, Issue 2, -p.1-8, (2020).
7. Butnaru, A., Mylonas, A., Pitropakis, N. Towards Lightweight URL-Based Phishing Detection. Future Internet, (2021), Vol 13, 154, p.1-15.
8. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Available at: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng
9. Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA. Available at: https://eur-lex.europa.eu/eli/dir/2019/713/oj/eng
10. Fan, Z., *et. al.*, Investigation of Phishing Susceptibility with Explainable Artificial Intelligence. Future Internet, (2024), Vol 16, 31, -p.1-18.
11. German Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by Article 2 of the Act of 22 November 2021 (Federal Law Gazette I, p. 4906), Available at: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html
12. Ike Vayansky and Sathish Kumar. Phishing – challenges and solutions. Computer Fraud & Security. (2018). -p. 15-20.
13. "Karistusseadustik (Penal Code), in RT I 2001, 61, 364 (in Estonian)." Available at: https://www.riigiteataja.ee/en/eli/522012015002/consolide
14. Kibercinayətkarlıq haqqında Budapeşt Konvensiyası. (2001). https://e-qanun.az/framework/18619
15. Kikerpill, K., and Siibak, a. Living in a spamster's paradise: deceit and threats in phishing emails. Masaryk University Journal of Law and Technology, - 2019, p.45-66.
16. Kim T.H.; Reeves, D.A survey of domain name system vulnerabilities and attacks. J. Surveill. Secur. Saf. 2020, 1, -p.34-60.
17. Lacey, D., and *et., al.* Taking the bait: a systems analysis of phishing attacks. 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE, - 2015, pp. 1109 – 1116.
18. Marc A. Rader, Syed (Shawon) M. Rahman. Explorıng Hıstorıcal And Emergıng Phıshıng Technıques

And Mıtıgatıng The Associated Securıty Rısks. International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.4, (2013).-p.23-41.

19.Muhammad Syafiq, *et.al.*, Phishing Attacks: Unraveling Tactics, Threats, and Defenses in the Cybersecurity Landscape. Available from: https://www.techrxiv.org/users/713944/articles/698221/master/file/data/CSC662_Written_Assignment_2022949945_MuhammadSyafiqBinKheruddin/CSC662_Written_Assignment_2022949945_MuhammadSyafiqBinKheruddin.pdf

20.Sandeep S. Parwe, Antonette R.Muntode. An Overview on Phishing- its types and Countermeasures. International Journal of Engineering Research & Technology (IJERT) Vol. 8 Issue 12, (2019). -p.545-548.

21.Shyni S., Adolphine A., and *et. al.,* "Phish Defender: Real-Time Detection Of Phishing Websites Using A Browser Extension". Metallurgical and Materials Engineering, (2025), p.1109-1117.

22.Stamm S., Ramzan Z., and Jakobsson M. Drive-By Pharming. Conference: Information and Communications Security, 9th International Conference, ICICS 2007, Zhengzhou, China, - 2007, -p.1-13.

23.Toapanta F., and *et.,al.* AI-Driven Vishing Attacks: A Practical Approach. The XXXII Conference on Electrical and Electronic Engineering, Eng. Proc.77, 15, - 2024, -p.1-10.

24.United Nations Convention Against Transnational Organized Crime and The Protocols Thereto. UNITED NATIONS, New York, 2004. Available at: https://l24.im/KrSO

25.https://scis.gov.az/az/news/view/39/umumi-kiberhucumlarin-91-ni-fisinq-hucumlari-teskil-edir

26.https://www.weforum.org/reports/global-cybersecurity-outlook-2025

27.https://www.cert.gov.az/news/2024-cu-il-erzinde-dovlet-qurumlarinin-informasiya-tehlukesizliyinin-temin-edilmesi-ucun-ehemiyyetli-tedbirler-gorulmusdur-8470?utm

28.https://cert.gov.az/az/news/suni-intellekt-gmail-de-olan-spam-ve-fisinq-mektublarin-99-ni-blok-edir?utm

29.https://medium.com/@alexandre.j_37811/phishing-attacks-part-1-b1ecef36a2e5

30.https://www.valimail.com/resources/guides/guide-to-phishing/phishing-vs-pharming/

31.https://expertinsights.com/insights/phishing-vishing-smishing-whaling-and-pharming-how-to-stop-social-engineering-attacks/

32.https://gointernos.com/phishing-smishing-vishing-pharming/

Камран ХАЛИЛОВ

СПОСОБЫ СОВЕРШЕНИЯ ФИШИНГОВЫХ АТАК В СРЕДЕ КИБЕРПРЕСТУПНОСТИ И ПРАВОВЫЕ ОСНОВЫ БОРЬБЫ С НИМИ

РЕЗЮМЕ

В современном цифровом мире число киберпреступлений, угрожающих государственным институтам, обществу и жизни отдельных людей, продолжает расти. Одной из таких киберугроз являются фишинговые атаки, с которыми мы часто сталкиваемся в своей повседневной жизни. Фишинговые атаки, которые чаще всего используются киберпреступниками, а также представляют большую угрозу для всех пользователей Интернета и трудно поддаются обнаружению, обуславливают необходимость совместного сотрудничества правоохранительных органов и граждан. Хотя фишинг может показаться одним из самых примитивных и удобных методов кражи информации у людей на начальном этапе, он имеет потенциал причинения вреда, поскольку является многогранным и не требует высокого профессионализма. Он используется для получения широкого спектра личной информации.

В этой связи важно знать криминальные характеристики фишинговых атак и предусматривать возможные меры против них. В данной статье объясняется степень общественной опасности путем определения характеристик фишинговых атак как вида киберпреступности. Также посредством данного исследования представлены соответствующие предложения по принятию адекватных мер против фишинговых атак в рамках борьбы с киберпреступностью.

Ключевые слова: фишинг, киберпреступность, атака, угроза, электронная почта.

Kamran KHALILOV

METHODS OF COMMITTING PHISHING ATTACKS IN THE CYBERCRIME ENVIRONMENT AND THE LEGAL BASIS FOR COMBATING THEM

SUMMARY

In the modern digital world, the number of cybercrimes threatening state institutions, societies and the lives of individuals continues to grow. One of these cyber threats is Phishing attacks, which we often encounter in our daily lives. Phishing attacks, which are most often used by cybercriminals and also pose a great threat to all Internet users and are difficult to detect, necessitate the joint cooperation of law enforcement agencies and citizens. Although phishing may seem like one of the most primitive and convenient methods of stealing information from people at the initial stage, it has the potential to cause harm because it is multifaceted and does not require high professionalism. It is used to obtain a wide range of personal information.

In this regard, it is important to know the criminal characteristics of phishing attacks and provide possible measures against them. This article explains the degree of public danger by defining the characteristics of phishing attacks as a type of cybercrime. Also, through this study, appropriate proposals are presented for taking adequate measures against phishing attacks within the framework of combating cybercrime.

***Key words**:* phishing, cybercrime, attack, threat, email.