UOT 34:343.1. Cinayət mühakimə icraatı, s.130-136

RƏŞAD NURİYEV

Ədliyyə Nazirliyinin Məhkəmə Ekspertizası Mərkəzinin
Sənədlərin texniki ekspertizası şöbəsinin eksperti,
Məhkəmə Ekspertizası Mərkəzinin doktorantı

E-mail: nuriyev.reshad@justice.gov.az
DOİ: https://doi.org/10.64498/KYTP5030

BANK DƏLƏDUZLUQLARININ ARAŞDIRILMASINDA RƏQƏMSAL EKSPERTİZANIN XÜSUSİYYƏTLƏRİ

Açar sözlər: bank dələduzluğu, rəqəmsal ekspertiza, server, mobil cihazlar, rəqəmsal yaddaş daşıyıcıları, zərərvericilər, təhlil, kriptovalyuta, investisiya, reklam.
Keywords: bank fraud, digital forensics, server, mobile devices, digital storage media, malware, analysis, cryptocurrency, investment, advertising.
Anahtar kelimeler: banka dolandırıcılığı, dijital adli bilişim, sunucu, mobil cihazlar, dijital depolama ortamı, kötü amaçlı yazılım, analiz, kripto para, yatırım, reklamcılık.
Ключевые слова: банковское мошенничество, цифровая криминалистика, сервер, мобильные устройства, цифровые носители информации, вредоносное ПО, анализ, криптовалюта, инвестиции, реклама.

Müasir dövrdə bank sektorunun rəqəmsallaşması, elektron ödəniş sistemlərinin geniş yayılması və onlayn bank xidmətlərinin sürətli inkişafı, eyni zamanda yeni riskləri də ortaya çıxarır. Rəqəmsal iqtisadiyyatın əsas aparıcı sahələrindən biri olan bank sisteminə qarşı həyata keçirilən kiberhücumlar, dələduzluq və qeyri-qanuni maliyyə əməliyyatları son illərdə qlobal miqyasda ciddi təhlükə kəsb etməkdədir. Xüsusilə də mobil bankçılıq, kriptovalyuta əməliyyatları və transsərhəd ödənişlərinin artması nəticəsində dələduzluq halları daha mürəkkəb forma alır. Beynəlxalq sferada maliyyə dələduzları və fırıldaqçıları haqqında regional və yeni tendensiyalar haqqında "INTERPOL Qlobal Maliyyə Fırıldaqçılıq Qiymətləndirməsi"ndə [1] ətraflı məlumat verilib.

INTERPOL-un araşdırmalarında müəyyən edilmişdir ki, maliyyə dələduzluqlarının törədilməsində istifadə olunan çoxsaylı üsullar arasında şəxsiyyətə bürünmə dələduzluğu, investisiya dələduzluğu, romantik dələduzluq, əvvəlcədən ödəniş tələbi ilə edilən dələduzluq və şəxsiyyət dələduzluğu qlobal miqyasda ən geniş yayılmış və təhlükəli təhdidlərdir. Bunlar içərisində "şəxsiyyət dələduzluğu"na nəzər salsaq bu növün fərdin şəxsi məlumatlarının (istifadəçi adı və şifrələr, kredit kartı məlumatları, biometrik məlumatlar və s.) icazəsiz əldə keçirilməsi və istifadəsi ilə bağlı olduğunu və qanunsuz maliyyə qazancı əldə etmək məqsədi daşıdığını müşahidə etmək olar. Şəxsiyyət dələduzluğu sosial mühəndislik (məsələn, phishing, smishing, vishing, spoofing və s.), sistemə müdaxilə (zərərli proqram təminatı və ya hakerlik texnikaları vasitəsilə) və fiziki oğurluq üsulları ilə şəxsi məlumatlara çıxış yolu ilə həyata keçirilir. Şəxsiyyət dələduzluğu iki elementdən ibarətdir: bir tərəfdən, şəxsi məlumatların qanunsuz maliyyə qazancı məqsədi ilə əldə keçirilməsi üçün istifadə olunan texnika, digər tərəfdən isə bu məlumatların həmin məqsədlə istifadəsidir. Dələduzlar, şəxsi məlumatları oğurlanmış qurbanın birbaşa iştirakı olmadan da şəxsiyyət dələduzluğu törədə bilirlər. Maliyyə vəsaitlərinin oğurlanmasından əlavə, dələduzlar bir çox hallarda əldə keçirilmiş şəxsi məlumatları onlayn cinayət bazarlarında da satırlar. Bu şəxsi məlumatlar isə cinayətkarlar tərəfindən şəxsiyyət dələduzluğu törətmək, qurbanları təkrar hədəf almaq və digər dələduzluq növlərində, məsələn, romantik dələduzluqda istifadə olunan aldatma texnikalarını asanlaşdırmaq üçün əlavə istifadə olunur.

Bu kontekstdə, "rəqəmsal ekspertiza" (digital forensics) bank dələduzluqlarının araşdırılmasında mühüm əhəmiyyət kəsb edir. Rəqəmsal ekspertiza prosesi yalnız texniki izlərin toplanması və təhlilindən

ibarət olmayıb, həm də hüquqi çərçivədə sübutların qəbul olunmasını təmin edən kompleks yanaşmanı tələb edir. Bank serverlərindən və mobil qurğulardan əldə edilən məlumatların elmi əsaslarla araşdırılması, cinayət hadisəsinin zəncirvari ardıcıllığının qurulması və dələduzluq mexanizmlərinin aşkarlanması prosesin əsas məqsədlərindəndir.

Azərbaycan Respublikasında rəqəmsal ekspertiza sahəsi son illərdə intensiv inkişaf mərhələsinə qədəm qoymuşdur. Hüquq-mühafizə orqanlarının istintaq praktikasında, xüsusilə bank dələduzluqları ilə bağlı işlərdə rəqəmsal sübutların rolu dinamik olaraq artmaqdadır. Bununla yanaşı, beynəlxalq təcrübə göstərir ki, kibercinayətkarlıq transsərhəd xarakter daşıdığı üçün yalnız milli səviyyədə deyil, həm də regional və qlobal əməkdaşlıq çərçivəsində kompleks yanaşma tələb olunur.

Məqalənin məqsədi bank dələduzluqlarının araşdırılmasında rəqəmsal ekspertizanın əsas xüsusiyyətlərini vurğulamaq, nəzəri və praktiki aspektlər haqqında ümumi məlumatları qeyd etmək, ölkə təcrübəsində rastlaşılan əsas hallar haqqında məlumatlar vermək və qeyd olunan halları beynəlxalq təcrübə ilə müqayisəli şəkildə əlaqələndirmək, həmçinin tətbiq olunan metod və metodologiyaların istifadəsi ilə ortaya çıxan nəticələr və bu nəticələrə dair profilaktik tövsiyələr irəli sürməkdir.

Ölkəmizdə də xüsusilə son illərdə bank sektorunda rəqəmsal texnologiyaların dinamik tətbiqi nəticəsində dələduzluq hallarının yeni formaları da ortaya çıxmışdır. Mobil bankçılıq, internet bankçılığı və onlayn ödəniş platformalarının geniş istifadəsi kiberhücumların əsas hədəflərinə çevrilmişdir. Ölkədə bank dələduzluqlarının araşdırılması müxtəlif dövlət qurumlarının və xidmətlərin birgə fəaliyyəti ilə həyata keçirilir. Bu təşkilatlara hüquq-mühafizə orqanları, "cert" mərkəzləri, təhlükəsizlik xidmətləri və digərləri aiddir.

Qeyd olunan qurumlar tərəfindən bu növ hüquq pozuntularının aşkarlanması, hadisələr haqqında faktiki halların müəyyənləşdirilməsi və araşdırılması, hüquq pozuntularının qarşısının alınması üçün tədbirlərin görülməsi, vətəndaşların bu növ dələduzluqların qurbanı olmaması üçün maarifləndirmə tədbirlərinin həyata keçirilməsi, hüquq-mühafizə orqanlarına və digər qurumlara bu məsələlərlə mübarizə aparmaq üçün tövsiyələrin verilməsi və bu kimi digər işlər görülür.

Təcrübədə bank dələduzluqlarının araşdırılması üzrə rəqəmsal ekspertiza əsasən iki istiqamətdə aparılır:

1. Zərərçəkmiş şəxsin mobil cihazının ekspertizası – tətbiqlərin fəaliyyətinə, şübhəli proqram təminatına, şifrələmə və autentifikasiya mexanizmlərinə baxılır.

2. Bank serverlərinin ekspertizası – əməliyyat jurnalları (log), giriş və qeydiyyat cəhdləri, şübhəli IP ünvanlarla həyata keçirilmiş tranzaksiyalar və s. araşdırılır.

Ekspertizanın aparılması zamanı kompüter sistemlərindən və digər tədqiqat obyektlərindən əldə olunmuş rəqəmsal məlumatlarla beynəlxalq standartlara uyğun olaraq rəftar edilir. Məsələn, mobil cihazların və digər rəqəmsal yaddaş daşıyıcılarının tədqiqatı zamanı ISO/IEC 27037:2012. [2] standartında göstərilənlərə əməl olunmalıdır. Bu standartda "Təhlükəsizlik Texnikaları - Rəqəmsal Sübutların İdentifikasiyası, Toplanması, Əldə Edilməsi və Mühafizəsi üzrə Təlimatlar" əsas prioritet olaraq seçilmişdir.

Son illərdə təcrübədə müşahidə olunan tipik hallar arasında:

- Mobil tətbiqetmələr vasitəsilə ələkeçirmə - OTP (One Time Password) və 3DS (3D Secure) kodlarının ələ keçirilməsi;
- Saxta tətbiqlər, zərərli proqram təminatı vasitəsilə müştəri cihazlarına müdaxilə;
- Fişinq hücumları nəticəsində müştərilərin hesab məlumatlarının oğurlanması;
- Kriptovalyuta platformaları vasitəsilə oğurlanmış vəsaitlərin "yuyulması";
- Vishing, sosial mühəndislik və bu kimi digər metodlarla fərdi məlumatların ələ keçirilməsi kimi hallar yer alır.

Qeyd olunan hallar beynəlxalq təcrübədə də geniş şəkildə yayılmışdır. Bu hallar barədə Europol. Internet Organised Crime Threat Assessment (IOCTA) 2025 [3] hesabatında da ətraflı qeyd edilmişdir.

Qeyd olunan halların müəyyən edilməsi rəqəmsal ekspertizanın aparılmasının - bank serverlərinə baxış mərhələsi zamanı ortaya çıxır. Belə ki, server üzərində bankın əsas məlumat bazasına baxış zamanı istifadəçiyə aid cihazlar bölməsində müştərinin istifadəsində olmuş cihazdan əlavə olaraq bir və ya bir neçə fərqli cihazların mövcud olması ortaya çıxır. Tədqiqat zamanı aşkar olunan bu qeydlər araşdırılaraq həmin fərqli cihazlara dair mümkün ola biləcək bütün məlumatlar toplanılır və hadisə zənciri təhlil olunur. Təcrübədə rastlaşılan bəzi hallar üzərindən nümunələr verə bilərik. Belə ki, təcrübədə ən çox hallar bank müştərilərinin sosial şəbəkələrdə "investisiya platformaları", "bank reklamları", "online alış-veriş platformaları", "çatdırılma xidmətləri",

"işə qəbul", "mobil operator xidmətləri", "bank xidmətləri" kimi reklam, göstəriş və ya xidmət adı altında yayılan tələlərə düşmələridir. Bu kimi hallarda dələduz əsasən özünü qeyd olunan xidməti verən şirkət nümayəndəsi kimi tanıdaraq, fərdi məlumatları əldə edir, bəzi mexanizmlərlə müştərinin mobil cihazına qoşulur və öz dələduzluq əməlini həyata keçirir. Dələduzluq əməli bank tətbiqinin başqa cihazda aktivləşdirilməsi, kənardan müdaxilə ilə müştərinin cihazının idarə edilməsi və ya bilavasitə müştəriyə göstərişlər (əməliyyatların icra edilməsi, saxta linklərin açılması və s.) verilməsi ilə ola bilir.

Bank dələduzluqları ilə bağlı olan ekspertizanın əsas xüsusiyyətlərinə gəldikdə, bu növ tədqiqatlarda ilk olaraq hadisə zənciri qurulur. Bunun üçün dələduzluğun hansı metodla, hansı tarixlərdə, hansı şəxs və hesablarla bağlı olduğu haqda ilk təsəvvürlər yaratmaq üçün iddia ərizəsi və işin digər materialları ilə tanış olunur. Hadisə haqqında ümumi təsəvvür yarandıqdan sonra işin gedişatına uyğun olaraq müştəriyə məxsus mobil cihaz tədqiq olunur.

Mobil cihazda baş vermiş hadisə ilə bağlı bütün - mobil tətbiq məlumatları, istifadəçi jurnalı, cihaz hadisələri (cihazın sıfırlanması və s.) və bu kimi məlumatlar toplanılır.

Mobil cihaz tədqiq olunarkən, dələduzluq hadisəsinin baş verdiyi tarixlərə daha çox diqqət yetirilir. Belə ki, eyni və yaxın tarixlərdə cihazda anomal hərəkətlərin baş verib-verməməsi müəyyən edilir. Cihazdan əldə olunmuş məlumatlar xüsusi kriminalistik proqramlar vasitəsi ilə təhlil olunur. Mobil cihazda quraşdırılmış tətbiqlər, istifadə olunmuş hesablar, zaman qeydləri, veb baxış tarixçəsi, cihaz hadisələri və bu kimi önəm daşıyan məlumatlar araşdırılır.

Məlumat üçün qeyd olunur ki, mobil cihazlarda kənardan müdaxiləni həyata keçirmək üçün istifadə edilən bir sıra proqram təminatları və digər vasitələr vardır. Bu növ vasitələrin istifadəsi ehtimalını nəzərə alaraq, cihazın yaddaşında həmin növ proqram təminatlarının və rəqəmsal izlərin olub-olmaması yoxlanılır.

Daha sonra, növbəti tədqiqat mərhələsi olaraq bank serverinə baxış keçirilir. Bank serverinə baxış keçirilərkən əsasən aşağıda qeyd olunan məlumatlar toplanaraq tədqiqat aparılır.

- Hücumçunun istifadə etdiyi metodlar (fişinq, malware, sosial mühəndislik);
- Serverlərdə log faylları, autentifikasiya qeydləri, IP ünvanları və şəbəkə protokolları;
- Transaction logları* araşdırılaraq şübhəli əməliyyatların tarixi;
- "CMS ID" qeydləri ilə əməliyyatların hansı istifadəçi hesabı;
- "Log analizi" – şübhəli əməliyyatların vaxtı, istifadəçi adı və IP ünvanı;
- Pulların hərəkətinin, o cümlədən vəsaitin bankdan digər hesablara köçürülməsi.

Ekspert təcrübəsi göstərir ki, bank dələduzluqlarında əsas məqsəd vəsaitlərin qısa müddətdə oğurlanaraq təmizlənməsidir.

Bank dələduzluqlarının ekspertizasında əsas nəticələr, ekspertizanı təyin etmiş orqan tərəfindən ekspert qarşısında qoyulmuş suallara əsasən aparılan tədqiqat əsasında formalaşır. Əlavə olaraq, iş üçün əhəmiyyət kəsb edən digər hallar da araşdırılaraq tədqiqat zamanı əldə olunmuş bütün məlumatlar əsasında ekspert rəyi tərtib olunur. Bu növ hallar üzrə təyin olunmuş ekspertizalarda əsasən bank müştərisi tərəfindən hadisə olduğu zaman istifadə edilən mobil cihaza kiberhücumun olub-olmamasına dair izlər, baş vermiş pul itkisi (çıxarılması) ilə əlaqədar – vəsaitin məbləği, tarixlər, əməliyyatların sayı, əməliyyatların növü, tranzaksiya detalları, pul köçürülməsinin növü, təhlükəsizlik kodları haqqında və bu kimi digər məlumatlar aşkarlana bilir. Ekspertiza zamanı əldə olunmuş bütün rəqəmsal sübutlar dələduzluq halının araşdırılması üçün istifadə oluna bilər. Belə ki, "Avropa İttifaqının Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi"nin (ENISA) [5] elektron sübutlar haqqında eyniadlı təlimatında "elektron sübut" anlayışı müxtəlif mənbələrə görə izah olunmuşdur.

ENISA: Elektron və ya rəqəmsal sübutların müxtəlif tərifləri mövcuddur. Avropa Şurasının Kiber Cinayətkarlığa dair Konvensiyası (Budapeşt Konvensiyası) [4] elektron sübutları cinayət əməlindən əldə edilə bilən və elektron formada olan sübutlar kimi təsvir edir. ABŞ Ədliyyə Nazirliyi isə rəqəmsal sübutu "məhkəmədə əsas kimi istifadə oluna bilən, ikilik (binary) say sistemi formasında saxlanılan və ya ötürülən informasiya" olaraq müəyyənləşdirir. Bu tərif "Rəqəmsal sübutların ekspertizası: Hüquq-mühafizə orqanları üçün Təlimat" [9] sənədində qeyd olunub.

Ümumilikdə, rəqəmsal sübutların əksər tərifləri onu belə ümumiləşdirir ki, rəqəmsal sübut cinayətin törədilib-törədilmədiyini müəyyən etmək (və ya inkar etmək) üçün istifadə oluna bilən rəqəmsal məlumatlardır.

Elektron sübutların toplanması prosesi mövcud vəziyyətin qiymətləndirilməsini, sübut dəyəri

ola biləcək müvafiq məlumat mənbələrinin müəyyənləşdirilməsini və bərpasını əhatə edir. Lakin qiymətləndirmə zamanı bir neçə əsas məsələyə diqqət yetirilməlidir: vəziyyətin dərindən başa düşülməsi, istintaqın potensial biznes təsiri və biznes infrastrukturunun müəyyənləşdirilməsi.

Ölkə təcrübəsinə qayıtdıqda, bank dələduzluqlarının inkişafı və dəymiş zərərin həcmi haqqında təsəvvür yaranması üçün ötən il ərzində baş vermiş dələduzluqların növlərinə aid bir məlumata diqqət yetirək.

Belə ki, ötən il ərzində ən çox aşağıdakı dələduzluq üsullarından istifadə ilə hüquq pozuntuları həyata keçirilmişdir:

- Saxta linklər vasitəsilə;
- Alış-veriş elanı bəhanəsi ilə;
- Bank əməkdaşı adı ilə dələduzluq;
- Mobil cihaza müdaxilə;
- Bankomatdan pul çıxarmaq bəhanəsi ilə;
- Oğurlanmış və itirilmiş kartlardan istifadə;
- Lotoreya ve qumar oyunları adı ilə aldatma;
- Alış-veriş saytlarında dələduzluq;
- Telefon satışına görə;
- Avtomobil satışına görə;
- İşə düzəltmə vədi ilə;
- Kredit vədi ilə;
- Kirayə ev, avtomobil və digər xidmətlərə görə.

Son dövrlərdə ölkəmizdə bu növ dələduzluq hallarının artması ilə birlikdə, hüquq-mühafizə orqanları, təhlükəsizlik xidmətləri, həmçinin bank təşkilatları tərəfindən müvafiq tədbirlər görülür. O cümlədən, ölkədə kibercinayətlərin qarşısının alınması, informasiya təhlükəsizliyinin təmin olunması, bu növ hüquq pozuntularında cinayət çərçivələrinin formalaşdırılması üçün ali səviyyədə müvafiq islahatlar aparılır.

Qeyd olunan qanunvericilik aktlarına "Kibercinayətkarlıq haqqında" Konvensiyanın (Budapeşt Konvensiyası) ratifikasiya edilməsi, "Azərbaycan Respublikasının Cinayət Məcəlləsinin 30-cu fəslində kibercinayətlər haqqında dəyişikliklərin və əlavələrin edilməsi" haqqında Qanunu, "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyası"nı, "Fərdi məlumatlar haqqında" Qanunu, "Nağdsız hesablaşmalar haqqında" Qanunu misal gətirmək olar.

Hüquq mühafizə orqanları tərəfindən qeyd olunan hüquq pozuntularının qarşısının alınması üçün görülən tədbirlərdən birinə nəzər salaq. Belə ki, "DİN əməliyyat keçirib - İnformasiya sistemlərinə kiberhücumlar təşkil edən şəxs saxlanılıb" başlığı ilə Daxili İşlər Nazirliyinin rəsmi internet saytında paylaşılan məlumatda kompüter sistemlərinə qanunsuz müdaxilə etməklə vətəndaşlara məxsus fərdi məlumatları əldə edən şəxsin saxlanılması haqqında qeyd olunmuşdur. Xəbərin məzmununda qeyd olunur ki, Daxili İşlər Nazirliyi (DİN) tərəfindən kibertəhlükəsizliyin qorunması və kibercinayətlərə qarşı mübarizə tədbirləri davam etdirilir. Bu istiqamətdə Nazirliyin Kibercinayətkarlıqla Mübarizə Baş İdarəsi vətəndaşların onlayn dövlət xidmətlərindən yararlanmaq üçün ən çox istifadə etdikləri sistemlərin məlumat bazalarına edilən kiberhücumlara qarşı xüsusi əməliyyat keçirib. Tədbir zamanı kompüter sistemlərinə qanunsuz müdaxilə etməklə vətəndaşlara məxsus fərdi məlumatları əldə edən Bakı şəhər sakini H.M müəyyən edilərək saxlanılıb. H.M internet üzərindən xarici ölkə vətəndaşlarından ibarət kibercinayətkar dəstələrlə əlaqələr yaradıb onlar vasitəsi ilə Azərbaycan vətəndaşlarının fərdi məlumatlarının qorunduğu sistemlərin şifrələrini əldə edib mühafizə tədbirlərini pozmaqla həmin serverlərə daxil olub. Daha sonra isə o, "Telegram" və digər sosial şəbəkələrdə yaratdığı anonim səhifələr vasitəsilə şəxsi məlumatları satışa çıxarıb. H.M sosial şəbəkələrdə bir neçə müxtəlif nüfuzlu şəxsin fərdi məlumatlarını da paylaşaraq istənilən vətəndaş barədə informasiyanı pul müqabilində sata biləcəyi barədə reklam xarakterli elanlar da yerləşdirib. Bu şəxsin kibercinayət əməlləri ifşa olunduqdan sonra onun topladığı fərdi məlumatlar və müvafiq onlayn informasiya sistemlərinə qanunsuz girişi Baş İdarə əməkdaşları tərəfindən aradan qaldırılıb. Əldə edilən elektron sübutların ekspertizası nəticəsində H.M-in kompüter sistemlərinə qanunsuz müdaxilə etmə faktı bir daha təsdiqlənib. Faktla bağlı Cinayət Məcəlləsinin müvafiq maddəsi ilə cinayət işi başlanıb. H.M təqsirləndirilən şəxs qismində cəlb olunmaqla istintaq aparılıb və cinayət işi yekunlaşdırılaraq baxılması üçün məhkəməyə göndərilib. H.M ilə əlbir olan və xarici ölkələrdə gizlənən şəxslərin də saxlanılması istiqamətində həmin dövlətlərin polis qurumları ilə birgə əməliyyat-texniki tədbirlər davam etdirilir.

Beləliklə, qeyd olunan xəbərdən də aydın olur ki, bu növ hüquq pozuntularında vətəndaşlara dair hər hansı bir məlumatın əldə olunması da dələduzlar tərəfindən sözügedən əməllərin həyata keçirilməsində istifadə oluna bilər.

Kiberdələduzluqların qurbanı olmamaq və ölkədə baş verən bu növ dələduzluq hallarının

sayının azalmasında köməklik göstərmək üçün hər bir elektron xidmət istifadəçisinin və məhsul sahibinin aşağıda göstərilən profilaktik tövsiyələrə əməl etməsi məqsədəmüvafiq hesab edilir.

- Bank müştəriləri tərəfindən: mənbəyi məlum olmayan tətbiqlərdən istifadə etməmək, məlum olmayan wi-fi şəbəkələrinə qoşulmamaq, sosial şəbəkələrə qoşula bilmək üçün naməlum VPN-lərdən istifadə etməkdən çəkinmək, naməlum şəxslərdən gələn elektron poçtlara daha diqqətli yanaşmaq və əmin olmadığınız halda elektron poçtlarda göstərilənləri icra etməmək, fərdi və maliyyə məlumatları (şəxsiyyət vəsiqəsi məlumatları, bank kartı və bank hesabı nömrələri) sorğulayan naməlum elektron poçt, sms və zənglərə cavab verməmək, mobil bank tətbiqlərində "iki faktorlu autentifikasiya"nı aktivləşdirmək, şübhəli linklərə keçməmək, fişinq mesajlarına cavab verməmək, smartfonlarda yalnız rəsmi mağazalardan (mənbələrdən) proqram təminatı yükləmək, antivirus və təhlükəsizlik proqramlarını daim yeniləmək kimi təhlükəsizlik tədbirlərinə əməl olunmalıdır.

- Banklar tərəfindən: bankın prosessinq xidmətinin təşkil olunmasında, kart əməliyyatları tarixçələrinin, həmçinin verilənlər bazası qeydlərinin (mobil tətbiqin jurnal qeydləri, istifadəçi məlumatları, kredit müraciətləri zamanı göndərilən mesaj qeydləri və s.) müntəzəm olaraq arxivlənməsinə və təhlil olunmasına xüsusi diqqət göstərilməlidir. Real vaxt rejimində şübhəli əməliyyatların monitorinqi aparılmalıdır. Baş vermiş kiber dələduzluq hallarının statistik göstəriciləri analiz edilərək bank müştərilərinin bu cür hüquq pozuntuları zamanı zərər çəkməməsi üçün öncədən maarifləndirmə tədbirləri görülməlidir. Həmçinin, bank əməkdaşlarının maarifləndirilməsi üçün davamlı "kibertəhlükəsizlik təlimləri"nin təşkil olunması məqsədəuyğun hesab edilir.

Əlavə olaraq qeyd olunur ki, kiber dələduzluq zamanı sıfırlanmış, format edilmiş, həmçinin kiberhücuma digər yollarla məruz qalmış mobil cihaz istifadə edildikcə (yeni məlumatlar yazıldıqca) yaddaş strukturu dəyişərək, rəqəmsal izlərin silinməsinə səbəb olur. Belə ki, bu növ hüquq pozuntuları baş verərkən məlumatların yüksək həcmdə bərpasının mümkünlüyü üçün hadisə zamanı istifadə olunan cihazın hadisə baş verdikdən sonra istifadə olunmaması, birbaşa hüquq-mühafizə orqanına və ya məhkəməyə təqdim edilməsi məqsədəuyğundur.

Ədəbiyyat siyahısı:

1. Europol. Internet Organised Crime Threat Assessment (IOCTA), 2023.
2. ISO/IEC 27037:2012. Information technology Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence.
3. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2025.
4. Kibercinayətkarlıq haqqında Konvensiya, Budapeşt, 23.11.2001.
5. Electronic evidence - a basic guide for First Responders. The European Union Agency for Network and Information Security (ENISA).
6. Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyası.
7. Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86. National Institute of Standards and Technology.
8. FATF. Cyber-enabled Fraud and Money Laundering, 2021.
9. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.
10. "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu.
11. "Nağdsız hesablaşmalar haqqında" Azərbaycan Respublikasının Qanunu.

XÜLASƏ

Məqalədə rəqəmsallaşan bank sektorunda baş verən dələduzluq halları və onların araşdırılmasında rəqəmsal ekspertiza metodlarının rolu təhlil olunur. Müasir dövrdə mobil bankçılıq, kriptovalyuta əməliyyatları və onlayn ödəniş sistemlərinin geniş yayılması yeni növ kibertəhlükələr – xüsusilə şəxsiyyət dələduzluğu, fişinq, zərərli proqram təminatları və sosial mühəndislik kimi hücum metodlarının artmasına səbəb olmuşdur.

Məqalədə qeyd olunur ki, rəqəmsal ekspertiza yalnız texniki məlumatların toplanması deyil, həm də hüquqi sübutların toplanmasına yönəlmiş sistemli və standartlaşdırılmış tədqiqatdır. Araşdırmalarda zərərçəkmişin mobil cihazları və bank serverləri təhlil olunur, hadisə zənciri qurularaq əməliyyat detalları müəyyən edilir. Bu proses zamanı beynəlxalq standartlar, xüsusilə ISO/IEC 27037:2012, əsas götürülür.

Azərbaycan təcrübəsi də nümunə kimi göstərilərək, bu sahədə hüquq-mühafizə orqanlarının, bankların və "CERT" mərkəzlərinin fəaliyyəti, eləcə də maarifləndirici tədbirlərin əhəmiyyəti vurğulanır. Məqalə, həmçinin kiberdələduzluqların qarşısının alınması üçün vətəndaşlara və banklara profilaktik tövsiyələr təqdim edilir.

FEATURES OF DIGITAL EXPERTISE IN THE INVESTIGATION OF BANK FRAUD

RASHAD NURİYEV

Expert of the Department of Technical Expertise of Documents of the Forensic Science Center of the Ministry of Justice, PhD student of the Forensic Expertise Center

SUMMARY

The article analyzes fraud cases in the digitalized banking sector and the role of digital forensics methods in their investigation. The widespread use of mobile banking, cryptocurrency transactions, and online payment systems in modern times has led to the growth of new types of cyber threats - in particular, identity fraud, phishing, malware, and social engineering attack methods.

The article notes that digital forensics is not only a systematic and standardized study aimed at collecting technical information, but also legal evidence. The studies analyze the victim's mobile devices and bank servers, establish a chain of events, and determine transaction details. During this process, international standards, in particular ISO/IEC 27037:2012, are taken as a basis.

The Azerbaijani experience is also cited as an example, emphasizing the importance of the activities of law enforcement agencies, banks, and "CERT" centers in this area, as well as educational measures. The article also provides preventive recommendations to citizens and banks to prevent cyber fraud.

BANKA DOLANDIRICILIĞI SORUŞTURMALARINDA DİJİTAL UZMANLIĞIN ÖZELLİKLERİ

RASHAD NURİYEV

Adalet Bakanlığı Adli Uzmanlık Merkezi Belge Teknik Bilirkişi Dairesi Uzmanı, Adli Uzmanlık Merkezi Doktora Öğrencisi

ÖZET

Makale, dijitalleşen bankacılık sektöründeki dolandırıcılık vakalarını ve bu vakaların araştırılmasında dijital adli bilişim yöntemlerinin rolünü analiz etmektedir. Mobil bankacılık, kripto para birimi işlemleri ve çevrimiçi ödeme sistemlerinin modern zamanlarda yaygınlaşması, özellikle kimlik dolandırıcılığı,

kimlik avı, kötü amaçlı yazılım ve sosyal mühendislik saldırı yöntemleri olmak üzere yeni siber tehdit türlerinin ortaya çıkmasına neden olmuştur.

Makalede, dijital adli bilişimin yalnızca teknik bilgi toplamayı amaçlayan sistematik ve standartlaştırılmış bir çalışma değil, aynı zamanda hukuki deliller de içerdiği belirtilmektedir. Çalışmalar, mağdurun mobil cihazlarını ve banka sunucularını analiz eder, bir olay zinciri oluşturur ve işlem ayrıntılarını belirler. Bu süreçte, özellikle ISO/IEC 27037:2012 olmak üzere uluslararası standartlar esas alınmaktadır.

Azerbaycan deneyimi de örnek olarak gösterilmekte ve kolluk kuvvetlerinin, bankaların ve "CERT" merkezlerinin bu alandaki faaliyetlerinin ve eğitim tedbirlerinin önemi vurgulanmaktadır. Makale ayrıca vatandaşlara ve bankalara siber dolandırıcılığı önlemek için önleyici öneriler sunmaktadır.

ОСОБЕННОСТИ ЦИФРОВОЙ ЭКСПЕРТИЗЫ В РАССЛЕДОВАНИИ БАНКОВСКОГО МОШЕННИЧЕСТВА

РАШАД НУРИЕВ

Эксперт отдела Технической экспертизы Документов Центра Судебной Экспертизы Министерства Юстиции, докторант Центра Судебной Экспертизы

РЕЗЮМЕ

В статье анализируются случаи мошенничества в цифровом банковском секторе и роль методов цифровой криминалистики в их расследовании. Широкое распространение мобильного банкинга, криптовалютных транзакций и систем онлайн-платежей в современном мире привело к появлению новых видов киберугроз, в частности, мошенничества с использованием личных данных, фишинга, вредоносных программ и методов социальной инженерии.

В статье отмечается, что цифровая криминалистика — это не только систематическое и стандартизированное исследование, направленное на сбор технической информации, но и юридических доказательств. В ходе исследований анализируются мобильные устройства жертвы и банковские серверы, устанавливается цепочка событий и определяются детали транзакций. При этом за основу берутся международные стандарты, в частности ISO/IEC 27037:2012.

Также приводится в качестве примера опыт Азербайджана, подчёркивающий важность деятельности правоохранительных органов, банков и центров «CERT» в этой области, а также образовательных мер. В статье также даны профилактические рекомендации гражданам и банкам по предотвращению кибермошенничества.

Rəyçi: Məhkəmə Ekspertizası Mərkəzinin Sənədlərin texniki ekspertizası şöbəsinin rəisi, fizika-riyaziyyat üzrə fəlsəfə doktoru N.T.Pənahov

Təqdim edən: R.Ə.Nuriyev

Daxil olma tarixi: 02.09.2025

Təkrar işlənmə tarixi: göndərilməyib

Çapa imzalanma tarixi: 15.09.2025