ELEKTRON TİCARƏTDƏ KİBERHÜCUMLARIN TƏHLİLİ: AZƏRBAYCAN RESPUBLİKASI VƏ DİGƏR ÖLKƏLƏRİN HÜQUQİ YANAŞMALARI

KAMRAN XƏLİLOV*

Annotasiya

XXI əsrin reallığında informasiya texnologiyalarının sürətli inkişafı qlobal iqtisadiyyatda rəqəmsallaşma proseslərini stimullaşdıraraq ticarət sektorunda əsaslı dəyişikliklərə səbəb olmuşdur. Elektron ticarətin yüksəlişi nəticəsində fərdi məlumatların elektron mühitdə toplanması, saxlanması və emalı geniş miqyas almışdır. Bu proses, bir tərəfdən istehlakçılar üçün rahatlıq və əlçatanlıq yaratdığı halda, digər tərəfdən fərdi məlumatların təhlükəsizliyi sahəsində yeni və kompleks risklərin ortaya çıxmasına səbəb olmuşdur. Xüsusilə fərdi məlumatların geniş həcmdə emalı kibercinayətkarlar üçün əlverişli hədəflər yaratmış və elektron ticarət platformalarının müxtəlif tipli kibertəhlükələrlə qarşı-qarşıya qalmasına gətirib çıxarmışdır. Bu kontekstdə aparılan tədqiqat, elektron ticarət sektorunda fərdi məlumatların təhlükəsizliyini təhdid edən əsas risk faktorlarını və yayılmış kiberhücum üsullarını müəyyənləşdirir. Məqalədə sosial mühəndislik, fişinq, DDoS hücumları və zərərli proqram təminatları kimi metodların elektron ticarətə təsiri araşdırılır və bu risklərə qarşı tətbiq edilə biləcək qabaqlayıcı texnoloji və hüquqi tədbirlər təqdim olunur. Həmçinin tədqiqatda məlumat pozuntularının hüquqi nəticələri, şirkətlərin hesabatlılıq və məlumatların müdafiəsi üzrə öhdəlikləri və pozuntuların təsirindən irəli gələn reputasiya və iqtisadi itkilər qiymətləndirilmişdir. Tədqiqat çərçivəsində, həm doktrinal, həm də müqayisəli hüquq metodologiyası əsasında müxtəlif ölkələrin normativ-hüquqi bazaları, xüsusilə Avropa İttifaqının Ümumi Məlumatların Qorunması Qaydası (GDPR), ABŞ-nin Kaliforniya İstehlakçı Məlumatlarının Qorunması Aktı (CCPA) və Azərbaycan Respublikasının "Fərdi məlumatlar haqqında" Qanunu təhlil olunmuşdur. Müqayisə nəticəsində, bu normativ aktlar arasında məlumat emalı prinsipləri, məlumat pozuntularının bildirilməsi rejimləri, şəxsin razılığı, hüquqi məsuliyyət və sanksiya mexanizmləri baxımından nəzərəçarpacaq fərqlər müəyyən edilmişdir. Tədqiqatda xüsusi vurğu risk əsaslı yanaşmanın tətbiqinə və bu modelin həm informasiya təhlükəsizliyi siyasətlərinə, həm də milli hüquqi tənzimləmələrə inteqrasiya imkanlarına edilmişdir. Məqalənin elmi yeniliyi onun hüquqi və texniki yanaşmaları birləşdirərək kompleks və çoxsahəli bir təhlil təqdim etməsindən ibarətdir. Nəticə etibarilə, bu tədqiqat, elektron ticarət sektorunda kibertəhlükəsizliyin təmin olunması üzrə milli və beynəlxalq

* Doktorant / Cinayət prosesi kafedrası / Bakı Dövlət Universiteti / Azərbaycan Respublikası Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyasının müəllimi / email: kamran.khalilov.isa@bsu.edu.az

praktikalardan istifadə etməklə, normativ uyğunluq, hüquqi cavabdehlik və texniki dayanıqlılıq aspektlərində effektiv modelin formalaşdırılması üçün praktik və nəzəri tövsiyələr irəli sürür.

Açar sözlər: *kiberhücum, elektron ticarət, zərərli proqram, qanunvericilik bazası, təhlükəsizlik, tədbir, müdafiə, strategiya, hüquqi tənzimlənmə.*

I. Giriş

Müasir rəqəmsal dünyada informasiya və kommunikasiya texnologiyalarının sürətli inkişafı insanların gündəlik həyat fəaliyyətindən başlayaraq biznes əlaqələrindəki proseslərə qədər bir çox sahələrə təsir göstərmişdir. Müəssisələrin informasiya-kommunikasiya texnologiyaları infrastrukturu yaradılarkən nəzərə alınmalı olan ən mühüm elementlərdən biri təhlükəsizlikdir. Son illərdə aparılan araşdırmalar göstərir ki, biznes sahəsində həyata keçirilən kiberhücumlar nəticəsində maliyyə itkiləri ağlasığmaz məbləğlərə çatmışdır.

İnformasiyanın vacib sərvət hesab olunduğu indiki dövrdə şirkətin daxili və xarici məlumatlarının başqa şəxslərin əlinə keçməsi arzuolunmazdır. Bu çərçivədə, elektron mühitə ötürülən fərdi məlumatlar həm qanunla qorunmalı, həm də texniki fərdi məlumatların təhlükəsizliyi təmin edilməlidir. Elektron ticarətdə əldə edilən fərdi məlumatların və müştəri verilənlər bazalarının ölçüsünü nəzərə alsaq, kiberhücumlar şəxsi məlumatların təhlükəsizliyinə ən böyük təhlükə yaradır. Elektron ticarət sektorunun kiberhücumların hədəfinə çevrildiyi günümüzdə kiberhücumlar günü-gündən fərqlilik qazanır və elektron ticarət saytları qarşılaşdıqları kiberhücumlardan sonra istehlakçı məlumatlarından tutmuş, şirkətlərin kommersiya sirlərinə qədər çoxlu məlumat və maliyyə itkisi ilə üzləşirlər. Fərdi məlumatların pozulması həm biznes, həm də istehlakçılar üçün iqtisadi itkilərə səbəb olmaqla yanaşı, həm də fərdi hüquq və azadlıqlar üçün təhlükə yaradır. Fərdi məlumatları emal edən elektron ticarət müəssisələrinin qanunla müəyyən edilmiş öhdəliklərini yerinə yetirməməsi və ya lazımi mühafizəni təmin edə bilməməsi səbəbindən zaman-zaman mövcud təhlükəsizlik boşluqlarından kibercinayətkarlar tərəfindən məharətlə istifadə edilir.

II. Rəqəmsal ticarətdə fərdi məlumatlara qarşı həyata keçirilən kiberhücumların növləri

Rəqəmsal ticarət saytlarının internetdə fəaliyyət göstərməsi və işçilərinin bir çoxunun internetlə bağlı əməliyyatlar həyata keçirməsi müəssisələri elektron hücumların açıq hədəfinə çevirir. Bu kontekstdə istifadə edilən bir çox hücum metodları və modelləri vardır. Fişinq hücumları, zərərli proqramlar, xidmətin rədd edilməsi hücumları (DDoS), sosial mühəndislik hücumları, *Man in the middle* hücumları (MITM) bunlardan yalnız bəzilərdir. Kibercinayətkarlar bu hücum üsullarından istifadə etməklə daxil olduqları informasiya kommunikasiya sistemlərinə xeyli ziyan vurur, sistemi sıradan çıxarır və ya məhv edir, sistemin xidmət funskiyasını pozur və ya tərkibindəki məlumatları sızdırır. Dünya

İqtisadi Forumunun (WEF) 2022 Qlobal Risklər Hesabatına əsasən, rəqəmsal sistemlərdən asılılığın artması cəmiyyətləri dəyişmiş və kibertəhlükəsizlik təhdidləri gətirmişdir. Tədqiqat, 2024-cü ildə zərərli proqram təminatı ilə kiberhücumların 350% artdığını, *ransomware* hücumlarının 435% artdığını və cəmiyyətlərin bu təhdidlərin qarşısının alınmasında effektivlik və ya onlara cavab vermə sürətini geridə qoyduğunu bildirib. Kiberhücumların, əsasən, maliyyə, e-ticarət, dövlət və səhiyyə sektorlarına yönəldiyi müəyyən edilib [15]. Kiberhücumların qarşısının alınması səylərinin qeyri-adekvatlığı, aqressiv hücum üsullarının getdikcə dəyişməsi və kibertəhlükəsizlik üzrə mütəxəssislərin sayının azlığı mövcud riski daha da ciddiləşdirir.

Qeyd olunduğu kimi, rəqəmsal ticarət mühitində bir çox fərqli kiberhücum üsullarından istifadə edilir. Həmin hücumları, onların cinayətkar xarakteristikasını və törədilmə metodlarını aşağıdakı kimi qruplaşdıra bilərik:

I. Fişinq hücumları. Texnoloji terminologiyada "fişinq" ingiliscə balıqçılıq mənasını verən "fishing" sözünün ilk hərfinin "ph" hərfləri ilə əmələ gəldiyi "password harvesting fishing" ifadəsindən törəmişdir [8, s. 117]. Fişinq hücumları sosial mühəndislik proqramlarının köməyi ilə istifadəçiləri saxta məzmunla aldatmaq və ya inandırmaqla həyata keçirilir. Bu, istifadəçi adı, parolu, şəxsiyyət məlumatları və kredit kartı məlumatları kimi məlumatları ələ keçirmək üçün istifadə edilən hücum üsuludur. Fişinq hücumlarında insanlar diqqəti cəlb edən e-poçt və ya etibarlı qurumlardan və ya biznes sahiblərindən göndərilmiş kimi görünən və təcili və çox vacib məsələləri ehtiva edən mesajlardan istifadə etməklə əldə edilir [3, s. 110]. İstifadəçiyə göndərilən saxta e-poçt mesajlarında "təhlükəsizlik məqsədilə müştəri məlumatlarınızı yeniləyin", "qısa müddətə bu xidmətdən pulsuz yararlanmaq üçün klikləyin", "...ardıcıl əməliyyatınız təsdiqlənib. Əgər əməliyyat sizin deyilsə, bura klikləyin" kimi aldadıcı məlumatlar ehtiva edir. E-poçtda yerləşdirilmiş keçidlər vasitəsilə istifadəçilər müxtəlif texnikalarla hazırlanmış saxta sayta yönəldilir və onların şəxsiyyət nömrəsi, ad və soyadı, kart məlumatları, kart parolları və internet filial parolları əldə edilir. Hazırda informasiya texnologiyaları sayəsində rəsmi internet saytının dəqiq surətini yaratmaq mümkün olmuşdur. E-poçt vasitəsilə göndərilən linkdə saxta vebsayt ola bilsə də, e-poçtda zərərli proqramların ola biləcəyi ehtimalı da var. E-poçt məzmununda olan keçidlərə zərərli proqram yüklənir və istifadəçiyə bu sənədi öz kompüterinə endirməyə imkan verir. Ümumilikdə, sistemə yeridilmiş bu cür proqramların sistem mühafizə proqramını söndürmək, keyloggerlər sayəsində basılan hər düyməni aşkar etmək, hətta ekran görüntüsünü çəkərək parolları və şəxsi məlumatları qeyd etmək funksiyalarına sahib olduğu məlumdur [10, s. 71].

II. Zərərli proqram təminatı. Bu növ kiberhücumlar istifadəçilərin xəbəri və iradəsi olmadan məlumat sızdırmaq və ya sistemlərin zədələnməsi kimi səbəblərdən istifadə etdikləri kompüterlərə quraşdırılmış proqram təminatını nəzərdə tutur [28]. Məlumdur ki, pulsuz proqramlar təklif edən, ümumiyyətlə, mənşəyi bilinməyən veb-səhifələr, xüsusən də maliyyə məlumatları əldə etmək

üçün bu proqramlara casus proqramlar quraşdıraraq kompüter sistemlərinə daxil olurlar. Zərərli proqram təminatı sayəsində sistemlərə icazəsiz giriş əldə edilir, kritik və vacib məlumatların əldə edilməsi asanlaşır və məqsəd sistem daxilində məlumatları oğurlamaq, şifrələmək və ya silməkdir [37]. Təkcə 2023-cü ildə dünya üzrə 6,6 milyard zərərli proqram hücumu aşkar edilib və məlum olub ki, zərərli proqramlar kiberhücumların ən çox yayılmış növlərindən biridir [33].

Bu kontekstdə, şəxsiyyət, əlaqə və ödəniş məlumatlarına əlavə olaraq satın alınan xidmətin sifariş nömrəsi, qiyməti, səfərdə istifadə olunacaq avtomobil və gediş-gəliş məlumatları, kredit məlumatları, səyahət sığortasının alınıb-alınmadığına dair məlumatlar, saytdan istifadə məlumatları, hansı yoxlama addımının xətaya səbəb olduğuna dair məlumatlar kimi bir çox detallı informasiyanın əldə oluna biləcəyi müşahidə edilir. Müştərinin şəxsi məlumatları fırıldaqçılıq və ya müxtəlif cinayətlər üçün istifadə olunsa və ya satılsa da, alınmış mal və ya xidmətlərlə bağlı əhəmiyyətsiz görünən məlumatlar rəqib e-ticarət şirkətləri tərəfindən məlumat vermək və öz fəaliyyətlərini təkmilləşdirmək və ya qiymət siyasəti yaratmaq üçün istifadə edilə bilər. Zərərli proqramlar tez-tez digər kiberhücum üsullarını həyata keçirmək üçün bir pilləkən rolunu oynayır və kompüter şəbəkəsinə daxil olduqdan sonra müxtəlif növ hücumlar həyata keçirilə bilər. Elektron ticarətdə istifadə olunan zərərli proqram növlərindən daha çox Viruslar, Troyan atları, casus proqramları, ransomware və rootkitlər kimi tipləri misal çəkmək mümkündür.

III. DDoS hücumları. DOS (Denial of Service) Azərbaycan dilinə tərcümədə "xidmətin rədd edilməsi" deməkdir və bir qayda olaraq tək bir mənbədən gələn şəbəkə axınını yararsız hala çevirmək cəhdidir. DDoS (Distributed Denial of Service) hücumu azərbaycan dilinə tərcümədə "paylanmış xidmətdən imtina hücumu" kimi başa düşülür. DDoS hücumları DoS hücumlarından fərqli olaraq tək bir neçə mənbədən gələn şəbəkə axını yararsız hala çevirmək cəhdi kimi müşahidə olunur [39, s. 2]. DDoS hücumları şəbəkələrə, xüsusən də internet bankçılığı və e-ticarət platformalarına ən çox yayılmış kiberhücum növü kimi tanınır və kiberhücumçular tərəfindən məlumat oğurluğu və məlumat sızması kimi kiberhücumlar həyata keçirərkən diqqəti yayındırmaq və xüsusilə də sistem sındırıla bilmədikdə, sistemə zərər vermək kimi məqsədlər üçün istifadə edilə bilər [26].

Bu hücum, sistemin mövcud şəbəkə tutumunu aşan ani sorğular və ani qoşulma sorğuları ilə sistemin tutumunu dolduraraq onun işləməsini və xidmət göstərməsini əngəlləmək məqsədi daşıyır. Hədəf sistemin imkanlarını aşan xidmət sorğusu nəticəsində server digər sistemlərdən və ya kompüterlərdən gələn xidmət sorğularına cavab verə bilmir və normal xidmət göstərə bilmir. DDoS hücumları ilə bağlı istifadə edilən digər konsepsiya Botnet konsepsiyasıdır. Bəzən kibercinayətkarlar böyük bir bot şəbəkəsi qurmaqla müəyyən hücumların həyata keçirilməsini daha asan idarəolunan hala gətirən, eləcə də bir-birilə bağlı və mütəşəkkil bir quruluş yaradır. Bu zərərli proqrama yoluxmuş kompüter şəbəkələri "Botnet" adlanır. Botnet identifikasiyası "zombi

kompüterlər" və ya "kölə kompüterlər" adlanan kompüterlər tərəfindən qurulmuş bir şəbəkədir. Botnetlər zərərli proqram və ya spam tətbiq etmək və ya hücumları həyata keçirmək üçün istifadə edilən üçüncü tərəflər tərəfindən idarə olunan təhlükəyə məruz qalmış kompüterlərdən ibarətdir. Botnet kimi istifadə edilən bu kompüterlər əvvəlcədən quraşdırılmış proqramlar sayəsində lazım olduqda əmr yerinə yetirirlər. Hücumlar botnetlər vasitəsilə bir və ya bir neçə serverə yüklənərək həyata keçirilir və botnet server kompüterinə çoxsaylı sorğular göndərərək serveri işlək vəziyyətə salmağa çalışır. Zərərli proqramlar sayəsində bir çox kompüterlər bilmədən botnetə daxil edilə bilər və botnet hücumunda istifadə edilə bilərlər. Botnetə bənzər proqramlar istifadəçiyə göndərilən e-poçtlara əlavə edilmiş fayllar və ya mesaj məzmununda olan keçidlərə klikləməklə açılan veb-səhifələr və ya Troyan atı adlanan zərərli proqram vasitəsi ilə də ötürülə bilər [19, s. 4].

Elektron ticarət sahəsində fəaliyyət göstərən müəssisələrin Botnet hücumlarından əziyyət çəkməsinin əsas səbəbi rəqib şirkətlərin qiymətlərlə rəqabət aparmaq cəhdidir. Xüsusilə e-ticarət saytlarında inventar və qiymətlər haqqında məlumat almaq üçün e-ticarət saytlarını araşdıran botlar hazırlanır. Toplanmış məlumatlar rəqib şirkətlərə satıla bilər və təklif ediləcək mal və ya xidmətlər üçün qiymət siyasəti yaratmaq məqsədilə istifadə edilə bilər. Digər tərəfdən, real müştərilərin məhsulları almasının qarşısını almaq üçün botlar vasitəsilə bir çox məhsulu səbətə əlavə etmək olar. Avtomatik hücumlar inventarın süni tükənməsinə səbəb olduğu üçün satışları və marka dəyərini azalda bilir.

IV. Ortadakı adam hücumu (Man in the Middle Attack (MITM)). Bu növ kiberhücum, şəbəkə üzərində olan hədəf kompüter və ya mobil cihaz ilə şəbəkə cihazı arasına girərək həmin şəbəkədən məlumat toplamaq əsasında həyata keçirilir [4, s. 208]. Təcavüzkarın iki şəbəkə arasındakı əlaqəni dinləməsi və müxtəlif məlumatların ələ keçirilməsi də təcavüzkarın ünsiyyətdə hər hansı bir dəyişiklik edərək yanıltıcı ünsiyyət yaratmasına imkan verir. Bu hücumların ən bariz xüsusiyyətlərindən biri onların antivirus proqramı tərəfindən fərqinə varmadan istifadəçi məlumatlarını ələ keçirmə qabiliyyətidir. MITM hücumları ilə telefon viruslarından istifadə etməklə təhlükəsizlik təbəqəsi pozula bilər və autentifikasiya üçün istifadəçinin telefonuna göndərilən mesajlar ələ keçirilə bilər. Elektron ticarət sahəsində paylaşılan şəxsi məlumatları, parolları və bank məlumatlarını əldə etmək üçün kompüter şəbəkəsində bir istifadəçi və ya cihazı təqlid edən bu tip hücum daxilolma (login) və şəxsiyyət məlumatlarının dəyişdirilməsinə və ya pul köçürməsinə səbəb olaraq ciddi ziyan vura bilər [6, s. 53].

III. Əsas müdafiə strategiyaları və onların tətbiqi

Elektron ticarət mühitində baş verəcək kiberhücumlara qarşı tətbiq oluna biləcək əks tədbirləri ümumilikdə 2 qrupda birləşdirə bilərik:

Birinci qrup tədbirlər - Fişinq xarakterli elektron poçtlara qarşı diqqətli olmağı, çox faktorlu autentifikasiyanı (Multi-factor Authentication) aktiv

etməyi, qoruyucu proqram təminatlarından istifadəni və maarifləndirmənin artırılmasını tələb edir. Belə ki, PDF fayllarda, "Microsoft Office" sənədlərində, e-poçt vasitəsilə göndərilən ZIP[1] və ya RAR[2] fayllarında saxlanılan zərərli proqram təminatı kompüter şəbəkəsinə və sisteminə sıza bilər. Bu, giriş ekranın monitorinqindən tutmuş klaviatura hərəkətlərinin qeydə alınmasına qədər bir çox üsullarla təmin edilir [5, s. 12]. Bu zaman hansı e-poçtların e-poçt şəbəkəsinə daxil olub-olmamasına nəzarət edən təhlükəsizlik proqramından istifadə etmək faydalı olardı. Bu zaman "Mail Gateway"[3] proqram təminatı vasitəsilə e-poçtun istifadəçiyə çatdırılmasından əvvəl təhlükəsiz olub-olmaması müəyyən edilir, domen adı yoxlanılır və məzmunu qiymətləndirilir. Gələn e-poçt etibarsız və ya zərərli olarsa, e-poçt rədd edilir və ya blokadaya alınır. Bu yolla, zərərli məzmun ehtiva edən e-poçt məzmununun bloklanması, e-poçtdakı əlavələrin və URL-lərin yaxşı və ya zərərli kimi təsnifləşdirilməsi, e-poçtdakı qorunan məlumatların müəyyən edilərək icazəsiz şəxslərə və ya başqasına ötürülməsinin qarşısının alınması təmin edilir [31, s. 554].

Çoxfaktorlu autentifikasiya sistemləri, xüsusilə fişinq hücumlarına qarşı ən təsirli üsullardan biri hesab olunur. Çoxfaktorlu autentifikasiya ilə istifadəçidən sistemə daxil olarkən autentifikasiya baxımından iki və ya daha çox məlumat qatını (məsələn, mobil telefona SMS, barmaq izi, giriş şifrəsi/şəkillə göndərilən kod) daxil etməyi tələb edən sistem nəzərdə tutulur. Bir-birindən müstəqil olan autentifikasiya təbəqələrindən biri təcavüzkarlar tərəfindən pozulsa belə, digər təbəqəni pozmaq mümkün olmadığı üçün istifadəçi kiberhücumlardan qorunacaq [2, s. 123]. Belə ki, hər hansı istifadəçinin parolu müxtəlif vasitələrlə əldə edilsə belə, çoxfaktorlu autentifikasiya baş verməyəcəyindən hesaba daxil olmaq və ya kart məlumatlarına daxil olmaq mümkün olmayacaq.

Digər müdafiə strategiyalarından biri şəbəkədə baş verən kibertəhdidlərə qarşı tətbiq olunan kompleks tədbirlərdir. Bu məqsədlə, nəzərə alınması lazım olan ilk tədbir təhlükəsizlik divarları (Firewall) adlandırılan vasitədir. Bu texnoloji vasitə, qurumun və ya təşkilatın yerli şəbəkəsi ilə digər xarici şəbəkələr arasında keçid rolunu oynayan, əvvəlcədən müəyyən edilmiş qaydalar və prinsiplər əsasında şəbəkəyə daxil olan və gedən trafiki idarə edən, eləcə də müəyyən edilmiş siyasətlərə uyğun olaraq məlumatların ötürülməsinə icazə verən və ya bloklayan proqram və ya aparat sistemləri kimi müəyyən edilə bilər [17, s. 109]. Bu kontekstdə, etibarsız xidmətlərin süzgəcdən keçirilməsi, sistemə nəzarət olunan girişin təmin edilməsi, təhlükəsizlik zəifliyi olan xidmətlərin

[1] ZIP faylı - məlumatların itkisiz sıxılmasını dəstəkləyən arxiv fayl formatıdır. ZIP faylı sıxılmış ola biləcək bir və ya bir neçə fayl və ya qovluqdan ibarət ola bilər.

[2] RAR və ya WinRaR – verilənlərin sıxılmasını, xətaların düzəldilməsini və faylların yayılmasını dəstəkləyən xüsusi arxiv fayl formatıdır.

[3] Mail Gateway – Elektron poçt şlüzləri təşkilatları və ya istifadəçiləri daxili e-poçt serverlərini qoruyan bir e-poçt server növüdür. Bu server hər gələn və gedən e-poçtun keçdiyi bir şlüz rolunu oynayır.

şəbəkəyə daxil olub-çıxmasının qarşısının alınması ilə rabitə təhlükəsizliyinin təmin edilməsi hədəflənir. İnternetə çıxışda potensial problemlərin həlli üçün xüsusi olaraq hazırlanmış bu sistem şəbəkədən kənardan şəbəkənin içərisinə girişi idarə edir və icazəsiz şəbəkə trafikini müşahidə etdiyi an bloklayır [34, s. 51]. İcazəsiz istifadəçilərin şəbəkəyə daxil olmasının qarşısını almaqla sistem zərərli proqramlardan, fişinq və sosial mühəndislik hücumlarından və uzaqdan girişdən qorunur. Prinsipcə, təhlükəsizlik divarları təkcə şəbəkə hücumlarına qarşı deyil, həm də bütün hücum üsullarına qarşı kibertəhlükəsizliyin əsasını təşkil edir. Firewall ilə birlikdə istifadə olunacaq Virtual Şəxsi Şəbəkə (VPN - Virtual Private Network)[4] və Məzmun Filtri (Content Filtering)[5] kimi əlavə tədbirlərlə effektiv şəbəkə təhlükəsizliyini təmin etmək mümkündür. Məzmun filtrləmə üsulu, ümumiyyətlə, şirkətlərdə internet firewalllarının bir hissəsi kimi istifadə olunur və bu üsul, şirkət işçilərinin şirkətin informasiya sistemindən kənar istənilən sosial media platformasına girişini süzgəcdən keçirmək və bloklamaq üçün istifadə olunur. Bu yolla, müxtəlif proqram və ya texniki vasitələrlə daxil olmaq nəzərdə tutulan təhlükəli veb səhifələr və daxil olan e-poçtlar bloklanır [18, s. 845].

Bu istiqamətdə atılacaq addımlardan biri də hücumun aşkarlanması və qarşısının alınması sistemləridir ki, (Intrusion Detection System (IDS)) onlar təhlükəsizliyi təmin etmək məqsədilə insan faktoru səhvlərini aradan qaldırmaq üçün istifadə olunur. Onlar şəbəkəyə yönəldilmiş bütün trafiki aşkar etmək, məlumat paketinin məzmununu yoxlamaq və hücum aşkar edildikdə avtomatik olaraq verilən əmri yerinə yetirmək, onu qeyd etmək və administratora məlumat vermək üçün nəzərdə tutulmuşdur. Başqa sözlə desək, hər hansı bir hücumun olması baxımından kompüter şəbəkəsində fəaliyyətə nəzarət etmək, təhlükə və pozuntuları aşkar etmək üçün məlumat trafikinin yoxlanılmasına və təhlilinə imkan verən bütün sistemlərdir [16, s. 24]. Müdaxilənin aşkarlanması sisteminə verilən əmr əlaqəni tamamilə kəsmək və ya bu əlaqəni kəsə biləcək başqa bir cihaza xəbərdarlıq etmək, sistem administratoruna məlumat vermək və hesabat vermək kimi hərəkətlər ola bilər. Mənbə ilə hədəf arasında birbaşa əlaqə yoluna yerləşdirilən bu sistem şəbəkə trafikində əvvəllər yaradılmış hücum imzalarına uyğun gələn hərəkətləri izləyir və hər hansı hücum zamanı trafiki bloklamaq xüsusiyyətinə malikdir [4, s. 196].

Müdafiə strategiyasına daxil olan növbəti addım kimi, DDoS hücumlarına qarşı görüləcək tədbirləri sadalamaq mümkündür. DDoS hücumlarında serverlər, ümumiyyətlə, böyük yüklə üzləşdiyindən bu yük,

[4] VPN - əlaqəni server vasitəsilə yönləndirərək və onlayn əməliyyatları gizlədərək internetə təhlükəsiz çıxışı təmin edən xidmətdir. Bu, ötürülən məlumatları şifrələməklə təhlükəsiz rabitə təmin etmək məqsədi daşıyır.

[5] Məzmun filtrasiyası adətən şirkətlərdə internet firewalllarının bir hissəsi kimi istifadə olunur. Bu üsul şirkət işçilərinin şirkətin informasiya sistemindən kənar istənilən sosial media platformasına girişini filtrləmək və bloklamaq üçün istifadə olunur. Bunlar müxtəlif proqram və ya aparatlarla əldə edilən veb səhifələri və daxil olan e-poçtları süzgəcdən keçirən sistemlərdir.

serverlərin adekvat və lazımi cavab verməsinin qarşısını alır. Bu səbəbdən, Yük tənzimləməsi (Load Balancing) adlanan üsuldan istifadə vacibdir. Bu üsulla şəbəkə və ya proqram trafiki server mühitində çoxlu serverlər arasında paylanaraq daha sağlam bir axın təmin edilir. Serverdəki yük artdıqca, Load Balancer işə düşür və trafik serverlər arasında paylanır. Beləliklə, DDoS hücumları kimi zərərli trafik ictimai bulud provayderinə yönəldilir və süzülür, şəbəkə sisteminə yeni təhlükəsizlik qatı əlavə edilir [11, s. 131]. Bu üsul, həm də e-ticarət sahəsində fəaliyyət göstərən şirkətlər tərəfindən mal və xidmətlərin satışı zamanı internet saytlarında sıx trafikin qarşısını almaq və daha yaxşı istifadəçi təcrübəsini təmin etmək üçün istifadə olunur [41, s. 1806].

Digər bir addım isə "Məzmun Çatdırılma Şəbəkəsi" (Content Delivery Network) adlanan metod adlanır. Bu metod, veb-sayta daxil olmaq istəyən istifadəçiləri onlara ən yaxın olan serverlərə yönləndirən və bu serverlər vasitəsilə xidmət almağa imkan verən server şəbəkə sistemindən istifadədir. Fayllar istifadəçiyə ən yaxın yerdəki server vasitəsilə dünyanın müxtəlif yerlərindən istifadəçi sorğularına göndərilir. Bu yolla sorğular paylanacağı üçün istənilən məkanda server daha az sorğu qəbul edir və yükləmə problemlərinin qarşısı alınır. Paylanmış şəbəkə strukturu sayəsində veb-saytların DDoS hücumlarına məruz qalmasının qarşısı alınır, hücum trafiki effektiv şəkildə idarə olunur və serverlər normal trafiklə təmin edilir. Bundan əlavə, DDoS hücumları süni intellekt və maşın öyrənmə texnologiyalarından istifadə etməklə aşkarlana və ya azaldıla bilər. Süni intellekt normal şəbəkə trafiki ilə DDoS hücum trafiki arasındakı fərqi öyrənməklə daim təkmilləşir.

İkinci qrup tədbirlər - Elektron ticarət mühitində baş verəcək kiberhücumlara qarşı tətbiq oluna biləcək əks tədbirlərin ikinci qrupu ödəniş sistemləri ilə bağlıdır. Belə ki, Elektron ticarət mühitində paylaşılan əsas şəxsi məlumatlar istifadəçilərin kredit kartı məlumatlarıdır. Bir çox istifadəçi kredit kartı məlumatlarının oğurlanması nəticəsində yaşayacaqları iqtisadi itki səbəbindən kredit kartı məlumatlarını paylaşmaqda tərəddüd edir [29, s. 355]. Kiberhücumlar nəticəsində əldə edilən kredit kartı məlumatları qeyri-qanuni məqsədlər üçün istifadə edilə və ya qeyri-qanuni fəaliyyətlərin aparıldığı mühitlərdə satışa təqdim edilə bilər. Bu səbəbdən ödəniş üsullarının və kart məlumatlarının təhlükəsizliyini təmin etmək üçün müxtəlif təhlükəsizlik protokollarının, eləcə də hüquqi tənzimləmələrin tətbiqi zəruri olmuşdur.

Ödəniş zamanı istifadəçilər kredit kartı sahibinin adı, kartın nömrəsi, istifadə müddəti və kartın təhlükəsizlik kodu (CVV)[6] kimi bir çox məlumatları paylaşırlar. Bu məlumat paylaşıldıqdan sonra e-ticarət saytı müqavilə bağladığı

[6] CVV - Kart yoxlama dəyəri (CVV) və ya kartın doğrulama kodu (CVC) ödəniş kartının məzmununun kriptoqrafik bütövlüyünün yoxlanılmasıdır. Onun əsas funksiyası əməliyyatlar zamanı sizin, kart sahibinin fiziki karta malik olduğunuzu yoxlamaqdır.

maliyyə qurumunun sistemi vasitəsilə virtual POS terminala[7] çıxışı təmin edir, kart məlumatlarını daxil etməklə alış-veriş məbləği üçün ehtiyat əldə edir və ödənişin təsdiq edilib-edilməməsi barədə müştəriyə bildiriş göndərir [2, s. 36]. Məhz bu hissədə paylaşılan kredit kartı məlumatlarını qorumaq üçün e-ticarət saytlarında ödəniş sistemini yaradan proqram təminatı kredit kartı məlumatlarının təhlükəsiz ötürülməsini təmin edən əlavə təhlükəsizlik tədbirləri ehtiva etməlidir.

Elektron ticarət mühitində ödəniş sistemlərinin təhlükəsizliyini təmin etmək üçün bir çox proqramlar hazırlanmışdır. Bunlardan ikisi daha mühüm təhlükəsizlik protokolu hesab olunur. Bunlar "Secure Sockets Layer (SSL)" və "Secure Electronic Transaction (SET)" sistemləridir. SSL sertifikatı server və müştəri arasında təhlükəsiz (şifrələnmiş) əlaqə yaratmaq üçün istifadə edilən standart təhlükəsizlik protokoludur və azərbaycan dilinə "təhlükəsiz giriş təbəqəsi" kimi tərcümə edilə bilər. O, veb-saytın ziyarətçiləri arasında məlumat mübadiləsini şifrələmək və internet üzərindən təhlükəsiz məlumat rabitəsini təmin edərək veb-saytın şəxsiyyətini yoxlamaq üçün istifadə olunur. Bu sertifikatlardan təkcə onlayn ödənişlərdə deyil, həm də təhlükəsizlik tələb edən bütün növ mesajlaşmalarda istifadə etmək mümkündür [7, s. 332]. SSL ilə göndəriləcək məlumat göndərilməzdən əvvəl şifrələnir və sistem məlumatın yalnız ünvan sahibi tərəfindən öyrənilməsinə imkan verir. Köçürülən məlumatlar şifrələmə alqoritmlərindən istifadə etməklə mürəkkəb olduğundan, təcavüzkarların əlaqə üzərindən göndərilən məlumatları oxumasının qarşısı alınır. Beləliklə, üzv girişləri (istifadəçi adı və şifrə), kredit kartı əməliyyatları və ya digər maliyyə əməliyyatları zamanı məlumat ötürülməsi daha təhlükəsiz olur və şəxsi məlumatların təhlükəsizliyi təmin edilir. Müştəri məlumatlarının təhlükəsiz olmasını təmin etmək, veb-saytın sahibliyini yoxlamaq, təcavüzkarların saytın saxta versiyasını yaratmasının qarşısını almaq və istifadəçiləri əmin etmək üçün e-ticarət saytlarının SSL sertifikatı da olmalıdır. Çünki istənilən istifadəçinin başına gələ biləcək ən pis vəziyyətlərdən biri onların şəxsi və ya maliyyə məlumatlarının oğurlanmasıdır. Bu səbəbdən SSL sertifikatı, xüsusilə e-ticarət müəssisələri üçün əvəzolunmaz bir vasitədir [1, s. 454].

SET protokolu isə internet saytında edilən alış-verişdə kart və ödəniş məlumatlarının məxfiliyini, kartdan istifadə edən şəxsin əsl kart sahibi olub-olmamasını və iş yerinin bankla müqaviləsinin olub-olmamasını təmin edən protokoldur. Elektron ticarətdə əməliyyatların etibarlılığını təmin etmək üçün hazırlanmış SET məhdud anonimlik təmin edir. Satıcı yalnız sifariş məlumatını görə bilir və müştərinin şifrələnmiş məlumatını banka ötürür. Bank alqı-satqı müqaviləsinin predmeti olan mallarla bağlı heç bir məlumat əldə edə bilmədiyi halda satış qiyməti və satıcının bank əlaqəsi haqqında məlumatı olur [9, s. 7].

[7] POS terminal - ödəniş kartı vasitəsilə malların, iş və xidmətlərin dəyərinin ödə-nilməsi, valyuta mübadiləsi əməliyyatlarının aparılma-sı, habelə nağd pul vəsaiti-nin alınması üçün nəzərdə tutulmuş avadanlıq.

SET-in iş məntiqi araşdırıldığında, SSL-də olduğu kimi, e-ticarət istifadəçisi mal və ya xidmətin alınması üçün sifariş yaradır və ödəniş məlumatlarını sistemə daxil edir. Sistemə daxil edilmiş sifarişlə bağlı məlumat satıcının kompüterinə ötürülür. Eyni zamanda, sifariş və ödəniş məlumatları bir-birindən tamamilə ayrı şifrələnir və bu şifrələnmiş əməliyyatlar rəqəmsal imza ilə təsdiqlənir. Bu arada satıcının sistemi şifrələnmiş ödəniş məlumatlarına rəqəmsal imza əlavə edir və müvafiq bankın SET serverinə ötürür. Bankın serveri şifrələnmiş məlumatın şifrəsini açır və alıcının kredit kartı şirkətindən onlayn təsdiq tələb edir. Kredit kartı şirkəti bu əməliyyatı təsdiq edərsə, alıcının kredit kartı avtomatik olaraq debet edilir. Nəhayət, SET serveri satıcının sisteminə ödənişin edilib-edilməməsi barədə mesaj göndərir. Doktrinada SET-in xüsusi ödəniş sistemi olmadığı, yalnız kredit kartı əməliyyatları üçün şifrələmə standartı olduğu bildirilir [24, s. 55].

Təhlükəsiz ödəniş məqsədilə onlayn əməliyyatlar üçün hazırlanmış əlavə autentifikasiya sistemi olan "3D Secure" üsulundan da istifadə olunur. Bu sistem kredit kartı və debet kartı əməliyyatlarında kart sahibinin şəxsiyyətini yoxlamağa kömək edir. Sistem çərçivəsində elektron ticarət istifadəçilərinin onlayn ödəniş etmək üçün sadəcə kart məlumatlarını daxil etmələri kifayət deyil. Kart məlumatı yoxlanıldıqdan sonra istifadəçi öz bankının 3D Secure ekranına yönləndirilir və sistemdə qeydiyyatdan keçmiş telefon nömrəsinə göndərilən birdəfəlik şifrəni müəyyən edilmiş vaxt ərzində daxil etməsi gözlənilir. Bu sistem sayəsində həm üzv müəssisələr, həm də kart sahibləri kart saxtakarlığından qorunur. Bu gün alıcıların kredit kartı məlumatlarının banklardan və ya şirkətlərin internet saytından oğurlanmasının qarşısını almaq üçün SET Standardı 3D Secure sistemi ilə əvəz edilmişdir [29, s. 180].

IV. Xarici ölkələrin və Azərbaycan Respublikasının qanunvericiliyində elektron ticarətin kibertəhlükəsizlik məsələləri

Dünya təcrübəsi göstərdi ki, kibertəhlükəsizlik infrastrukturu olmadan elektron ticarətin təhlükəsizliyi və dayanıqlılığı istənilən səviyyədə təmin edilə bilməz. Dünyanın bir neçə inkişaf etmiş ölkələrində elektron ticarətdə tətbiq edilən modellər kibertəhlükəsizliyin qorunması baxımdan öz töhfələrini göstərə bilmişdir. Belə ölkələrdən biri kimi ABŞ-ni misal çəkə bilərik. Belə ki, ABŞ-də elektron ticarət sektorunda kibertəhlükəsizlik, hüquqi tənzimləmə baxımdan vahid və mərkəzləşdirilmiş qanunvericilik bazasına deyil, sektorial, könüllülük prinsipinə və çoxpilləli yanaşmaya əsaslanır. ABŞ modeli çevikliyi, texnoloji innovasiyaları təşviq etməyi və özəl sektorun özünü tənzimləməsini rəhbər tutur [14, s. 3].

Bu kontekstdə, müvafiq sahə üzrə bir sıra vacib qanunvericilik aktları qəbul edilmişdir. Bunlardan ən vacibləri olan "Kibertəhlükəsizlikdə məlumat paylaşılması aktı" (Cbyersecurity Information Sharing Act) və NIST-in kibertəhlükəsizlik çərçivəsi (NIST: Cybersecurity Framework) elektron ticarətin platformaları üçün texniki və hüquqi tələbləri formalaşdırır. Daha dəqiq desək, 2015-ci ildə qəbul edilmiş "Kibertəhlükəsizlikdə məlumat paylaşılması aktı"

özəl sektor və dövlət arasında kibertəhlükə məlumatlarının könüllü mübadiləsini təşviq edən ən vacib sənəddir. Bu sənəd elektron ticarət operatorlarına əvvəlcədən xəbərdarlıq və müdafiə tədbirləri üçün böyük imkanlar yaradır [36]. 2014-cü ildə ABŞ-nin Milli Standartlar və Texnologiyalar İnstitutu (NIST) tərəfindən hazırlanmış "Kibertəhlükəsizlik Çərçivəsi" isə şirkətlərə öz təhlükəsizlik səviyyələrini qiymətləndirmək və artırmaq üçün könüllü standartlar təqdim edir. Bu çərçivə 5 əsas funksional prinsipə əsaslanır: Risklərin müəyyən olunması (identify); təhlükəsizlik tədbirlərinin tətbiqi (protect); hücumların aşkarlanması (detect); hücumlara cavab (respond); bərpa və davamlılıq tədbirləri (recover) [25, Art. 2.2]. Elektron ticarət şirkətləri bu çərçivədən istifadə etməklə könüllü əsaslı uyğunluq nümayiş etdirir və bazar reputasiyasını qoruyur. Onu da qeyd etmək olar ki, ABŞ-də rəqəmsal ticarətə ümumi nəzarətin formalaşdırılması üçün müvafiq qurumların fəaliyyəti və səlahiyyətləri də dəqiq müəyyən edilmişdir. Belə ki, rəqəmsal istehlakçı hüquqlarının pozulması və ya məlumat pozuntusu hallarında şirkətlərin məsuliyyəti və reklam fəaliyyəti üzrə əsas nəzarətçi olaraq Federal Ticarət Komissiyası (Fedral Trade Comission) çıxış edir. Bu qurum illər üzrə hesabatlar tərtib etmək, pozuntu hallarını araşdırmaq və ticarət saytlarını cərimələmək kimi səlahiyyətlərə malikdir [32, s. 614].

ABŞ-dən fərqli olaraq, Çin kibertəhlükəsizlik sahəsində dövlət nəzarətinə əsaslanan, mərkəzləşdirilmiş və sərt tənzimləmə modelini tətbiq edir. Bu model, xüsusilə elektron ticarət sektorunda dövlətin məlumat axını və texnoloji infrastruktur üzərində ciddi nəzarəti təmin etməyə yönəlmişdir. Çin təcrübəsi suverenlik əsaslı kiberməkan siyasətinin hüquqi alətlər vasitəsilə reallaşmasının nümunəsidir. Bu ölkədə müvafiq sahəni tənzimləyən 3 əsas qanunvericilik aktını misal çəkmək mümkündür. Bunlardan birincisi, "Kibertəhlükəsizlik Qanunu" (Cybersecurity Law of the PRC (2017)) hesab olunur. Bu Qanun, Çində informasiya sistemlərinin və rəqəmsal platformaların təhlükəsizliyinə dair əsas hüquqi akt sayılır. Qanunun ümumi məzmunundan belə başa düşülür ki, elektron ticarət subyektləri kritik informasiya infrastrukturuna daxil olduqda dövlətin xüsusi tənzimləməsinə tabe olurlar. İstifadəçi məlumatlarının Çində lokal serverlərdə saxlanılması məcburi hesab olunur. Bununla yanaşı, təhlükəsizlik auditi və sertifikatlaşdırma prosedurları məcburidir [27]. Digər iki normativ sənəd "Məlumat Təhlükəsizliyi" (Data Security Law (2021)) və "Şəxsi məlumatların qorunması Qanunudur (Personal Information Protection Law (2021)). İlk qanun müvafiq olaraq məlumatların kateqoriyalara ayrılmasını və onlara uyğun təhlükəsizlik tədbirlərinin tətbiqini tələb edir və "Əhəmiyyətli məlumat" və "əsas milli məlumat" kimi kateqoriyalar fərqli hüquqi rejimlərə tabe edilir. Həmçinin məlumatın xarici tərəflərlə paylaşılması üçün dövlətin öncədən razılığı tələb olunur [23, s. 214]. Digəri isə, Avropa İttifaqının GDPR modeli əsasında hazırlanmış olsa da, daha sərt dövlət nəzarəti mexanizmlərini ehtiva edir. Belə ki, həmin qanunda fərdi məlumatların emalı üçün hüquqi əsaslar, istifadəçinin açıq razılığı və məqsəd-məhdudiyyəti prinsipi müəyyənləşdirilmişdir. Əlavə olaraq,

məlumatların Çin xaricinə ötürülməsi üçün təhlükəsizlik qiymətləndirməsi, müqavilə və ya dövlətin təsdiqi tələb olunur [40, s. 37].

Avropa İttifaqı elektron ticarət sahəsində kibertəhlükəsizliyin təminini şəxsi həyatın toxunulmazlığı, rəqəmsal hüquqlar və rəqəmsal infrastrukturun etibarlılığı çərçivəsində həyata keçirir. Avropa İttifaqının hüquqi yanaşması risk əsaslı, prinsiplərə əsaslanan və texnoloji neytral tənzimləmə modelinə söykənir. 2016-cı ildə qəbul edilən "Şəbəkə və İnformasiya Sistemlərinin Təhlükəsizliyi üzrə Direktiv" (NIS), Avropa İttifaqında kibertəhlükəsizlik sahəsində ilk normativ sənəd kimi çıxış etmişdir. Direktivin məqsədi əsas xidmət operatorları və rəqəmsal xidmət təminatçılarının kibertəhlükəsizlik tədbirləri görməsini və insidentləri bildirməsini tələb etməklə vahid təhlükəsizlik səviyyəsi yaratmaq olmuşdur. Daha dəqiq desək, həmin sənədlə hücum və insidentləri müvafiq milli orqanlara 24 saat ərzində bildirmək öhdəliyini müəyyən edilmişdir [12].

2022-ci ildə qəbul edilən NIS2 Direktivi (EU) 2022/2555 bu sahədə öhdəlikləri daha da sərtləşdirmiş, əhatə dairəsini genişləndirmiş və səlahiyyətli nəzarət orqanlarının fəaliyyətini gücləndirmişdir. NIS2 aşağıdakı yeni tələbləri ehtiva edir: elektron ticarət platformaları, onlayn bazarlar və axtarış sistemləri də "əhəmiyyətli və vacib qurumlar" kimi öhdəlik altına alınır; şirkətlər risk əsaslı texniki və təşkilati təhlükəsizlik tədbirləri qəbul etməli, illik təhlükəsizlik auditi aparmalıdırlar; direktiv idarə heyətinə birbaşa məsuliyyət yükləyir və ciddi sanksiyalar tətbiq edir [13].

Elektron ticarətdə fərdi məlumatların qorunması ən vacib məsələlərdən biridir. Bu baxımdan, Avropa İttifaqı özünün ən məşhur sənədi olan "Ümumi Məlumatların Qorunması Reqlamenti"ndə (GDPR) məsələyə olan mövqeyini açıq-aşkar ortaya qoymuşdur. GDPR bu sahədə qlobal miqyasda standartlaşmış hüquqi mexanizm təqdim edir. GDPR-in 32-ci maddəsinə əsasən, məlumatları emal edən istənilən təşkilat (o cümlədən elektron ticarət platformaları) aşağıdakı tədbirləri həyata keçirməlidir: məlumatın şifrələnməsi və ya psixoloji təhlükəsizliyi təmin edən texnologiyaların tətbiqi; daimi məxfilik, bütövlük və əlçatanlığın təmin edilməsi üçün sistem və xidmətlərin dayanıqlığı; fiziki və texnoloji insidentlər zamanı məlumatlara çıxışı və sistemin fəaliyyətini bərpa etmə qabiliyyəti; müntəzəm test və auditlər vasitəsilə tədbirlərin effektivliyinin qiymətləndirilməsi. Göründüyü kimi, bu yanaşma risk əsaslı modelə əsaslanır və təşkilat riskin səviyyəsinə görə tədbirləri müvafiq şəkildə planlaşdırmalıdır [38]. Bundan başqa, GDPR-in 33-cü və 34-cü maddələrinin məzmununa əsasən istənilən məlumat sızması baş verdikdə məlumatı emal edən təşkilat bu barədə 72 saat ərzində nəzarət orqanını məlumatlandırmalıdır. Əgər insident fərdi şəxslərin hüquq və azadlıqlarına yüksək risk yaradırsa, həmin şəxslər birbaşa xəbərdar edilməlidir. Nəzəriyyədə qeyd olunur ki, məhz bu üsul, yalnız mühafizəni gücləndirmir, həm də insidentlərə cavab verilməsini sürətləndirir və şəffaflığı artırır [35, s. 147]. Nəticə olaraq, Avropa İttifaqında elektron ticarətlə məşğul olan subyektlər üçün hüquqi tələblər aydın, texniki standartlar konkret və

nəzarət mexanizmləri təsirli şəkildə qurulmuşdur. Bu, həm istifadəçilərin etimadını artırır, həm də bazar iştirakçıları üçün ədalətli və təhlükəsiz mühit yaradır.

Azərbaycan Respublikasının qanunvericilik bazası rəqəmsal ticarət sahəsinin tənzimlənməsi üçün müxtəlif normativ mənbələri özündə cəmləşdirir. Biz bu mənbələri, ümumilikdə, 2 yerə bölə bilərik: Xüsusi (sahəvi) və Ümumi. Xüsusi qanunvericilik mənbələri məhz rəqəmsal ticarət sferasını, elektron müqavilələri, elektron imzanı, fərdi məlumatları, ödəniş vasitələrini və s. birbaşa tənzimləyən qanunvericilik aktlarıdır. Buraya "Elektron ticarət haqqında" Qanun (2005), "Elektron imza və elektron sənəd haqqında" Qanun (2004), "Fərdi məlumatlar haqqında" Qanun (2010), "Ödəniş xidmətləri və ödəniş sistemləri haqqında" Qanun (2023) və "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunlar (1998) aiddir. Qeyd edilən qanunlar birbaşa olaraq internet məkanında təhlükəsiz alış-veriş və ticarət fəaliyyətinin təmin edilməsinə istiqamətlənməsə də, ümumilikdə, ölkəmizdə müvafiq sahə üzrə bir çox qaydaların təşəkkül tapmasında və tətbiq mexanizmlərinin inkişaf etdirilməsində vacib rol oynayırlar.

Xüsusilə, "Elektron ticarət haqqında" Qanunun 6-cı maddəsində elektron ticarətin təhlükəsizliyinin təmin olunması dövlət siyasətinin əsas istiqamətlərindən biri kimi qeyd olunur və elektron müqavilələrin təhlükəsiz mühitdə bağlanmasını şərtləndirir. Həmçinin iştirakçılar arasında məlumatların dəyişməzliyi və bütövlüyü prinsipi tanınır. Bundan başqa, Qanunun mühüm elementlərindən biri elektron sənəd və elektron imza anlayışlarının hüquqi tanınmasıdır. Eyni zamanda, elektron müqavilələrin bağlanması zamanı tərəflərin identifikasiyası, məlumatların bütövlüyü və transaksiyaların təhlükəsizliyi qanun çərçivəsində prinsipial əhəmiyyət kəsb edir [20]. Ümumiyyətlə, Qanunun əsas məqsədi elektron mühitdə aparılan ticarət əməliyyatlarının şəffaf, təhlükəsiz və hüquqi baxımdan etibarlı şəkildə həyata keçirilməsini təmin etməkdir. Qanunla elektron ticarət iştirakçıları (satıcı və alıcı), onların hüquq və vəzifələri, əməliyyatların hüquqi nəticələri və dövlət orqanlarının rolu müəyyən edilir. Bu hüquqi çərçivə həm daxili ticarət münasibətlərinə, həm də transsərhəd e-ticarət əməliyyatlarına şamil edilə bilər. Qanunun digər mühüm komponenti elektron kommersiya bildirişləri və reklamlarının qanuni statusudur. Qanun kommersiya bildirişlərinin göndərilməsi zamanı istifadəçinin əvvəlcədən məlumatlandırılmasını və razılığının alınmasını tələb edir [20]. Bu, e-ticarətdə istifadəçinin hüquqlarının qorunması baxımından mühüm məsələdir və "Fərdi məlumatlar haqqında" Qanunla vəhdət təşkil edir. Bununla belə, sözügedən Qanunun bir sıra boşluqları da mövcuddur. Belə ki, BMT-nin UNCITRAL Model Qanunu, Avropa İttifaqının e-Commerce Directive və OECD prinsiplərinə nisbətən daha ümumi və prinsipial yanaşma sərgiləyir. Qanun müasir rəqəmsal texnologiyaların, o cümlədən mobil ticarət, bulud texnologiyaları, avtomatlaşdırılmış alqoritm əsaslı qərar qəbuletmə sistemləri və süni intellekt platformalarının hüquqi münasibətlərdə iştirakını əhatə etmir.

Azərbaycan Respublikasının "Fərdi məlumatlar haqqında" Qanunu rəqəmsal ticarət münasibətlərinin hüquqi tənzimlənməsində mühüm normativ-hüquqi baza təşkil edən sahəvi aktlardan biridir. Elektron ticarət çərçivəsində fərdi məlumatların toplanması, emalı və saxlanması prosesi geniş vüsət aldığından, bu sahədə şəxsin informasiya təhlükəsizliyinin və şəxsi həyat toxunulmazlığının qorunması məsələləri istər-istəməz aktuallıq qazanır. Qanun məhz bu ehtiyaclara cavab vermək məqsədi daşıyır və rəqəmsal iqtisadiyyatın əsas təməl daşlarından biri kimi çıxış edir. Qanuna əsasən, fərdi məlumatlar yalnız məlumat subyektinin razılığı ilə, qanuni və konkret məqsədlərlə toplanmalı, üçüncü şəxslərə ötürülməsi hallarında isə əlavə razılıq tələb olunmalıdır. Elektron ticarət sahəsində bu prinsip, xüsusilə əhəmiyyətlidir, çünki onlayn mağazalar, ödəniş sistemləri, mobil tətbiqlər və müxtəlif xidmət platformaları istifadəçilərdən geniş həcmdə şəxsi məlumatlar (ad, soyad, ünvan, ödəniş vasitələri, IP ünvanı, lokasiya məlumatları və s.) toplayır. Bu məlumatların emalı zamanı qanunun müəyyən etdiyi "məqsədyönlülük", "qanunauyğunluq", "məhdudiyyət" və "məlumat subyektinin məlumatlandırılması" prinsipləri tətbiq olunmalıdır [21].

Qanun həmçinin fərdi məlumatların təhlükəsizliyinə dair ümumi tələblər irəli sürür. Belə ki, fərdi məlumatların mühafizəsi məqsədilə məlumatı emal edən subyekt (yəni satıcı, platforma sahibi və ya xidmət təminatçısı) texniki və təşkilati tədbirlər görməlidir. Lakin qanunda bu tədbirlərin konkret texniki spesifikasiyası göstərilmir və beynəlxalq standartlarla (məsələn, ISO 27001 və ya GDPR) uyğunluq səviyyəsi aşağıdır. Məlumatların şifrələnməsi, müntəzəm təhlükəsizlik yoxlamaları, kibertəhlükəsizlik insidentlərinə dair xəbərdarlıq öhdəlikləri kimi müasir yanaşmalar qanunda açıq şəkildə öz əksini tapmamışdır.

Sahəvi qanunlardan biri kimi, "Ödəniş xidmətləri və ödəniş sistemləri haqqında" Qanunu, əsasən, ödəniş xidmətlərinin göstərilməsi, ödəniş sistemlərinin təşkili və iştirakçıların hüquq və vəzifələri ilə bağlı normativ çərçivəni müəyyənləşdirir. Əsas məqsəd, rəqəmsal ticarətdə istifadə olunan ödəniş mexanizmlərinin təhlükəsizliyini təmin etmək, maliyyə texnologiyalarının tətbiqini stimullaşdırmaq və istifadəçilərin hüquqlarını müdafiə etməkdir. Qanun həm də rəqəmsal ticarətdə real vaxtlı ödəniş sistemləri, mobil və elektron cüzdanlar, rəqəmsal bankçılıq xidmətləri, eləcə də ödəniş vasitələrinin innovativ formaları üçün hüquqi zəmin yaradır. Rəqəmsal ticarət mühitində bu qanunun mühüm rolu odur ki, o, satıcı ilə alıcı arasında ödəniş əməliyyatlarının hüquqi əsaslarını sistemləşdirir. Xüsusilə də onlayn ticarətdə geniş istifadə olunan bank kartı, elektron pul, mobil ödəniş və internet bankçılıq vasitələrinin hüquqi statusu, onların istifadəsi zamanı məlumatların mühafizəsi, istifadəçinin razılığı və əməliyyatların geri qaytarılması prosedurları aydın şəkildə tənzimlənmişdir. Qanunun bir digər önəmli elementi ödəniş əməliyyatlarında şəffaflıq və informasiyanın açıqlanması prinsipidir. Xidmət göstərən tərəf (məsələn, elektron ticarət platforması və ya ödəniş təşkilatı) istifadəçini əməliyyat xərcləri, müddətlər və konvertasiya şərtləri barədə

əvvəlcədən məlumatlandırmalıdır [22]. Bu yanaşma, istifadəçi hüquqlarının qorunması baxımından beynəlxalq maliyyə xidmətləri standartlarına uyğunluq niyyəti ilə səsləşir.

İkinci qrup qanunlara ümumi olaraq rəqəmsal ticarətə dolayı tətbiq edilən və ya ümumi ticarət münasibətlərinə aid edilə bilən normativ sənədlər daxildir. Bunlar əsaəsn, Mülki Məcəllə (elektron müqavilə hüququ, məsuliyyət məsələləri), Vergi Məcəlləsi (ƏDV, elektron xidmətlər üzrə məsələlər), Gömrük Məcəlləsi (elektron idxal/ixrac məsələləri), İnzibati Xətalar və Cinayət Məcəllələri (kibercinayətlər, məlumat sızması məsələləri) və müvafiq sahə üzrə Azərbaycan Respublikası Prezidentinin Fərman və Sərəncamlarıdır. Bunlardan ən vacibi kimi "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyası"nın təsdiq edilməsi haqqında" Sərəncamı qeyd etmək olar. Bu sənəd elektron ticarət platformalarının texniki müdafiə səviyyəsinin artırılması, kibertəhlükəsizlik insidentlərinin aşkarlanması və cavab sistemlərinin formalaşdırılması, elektron identifikasiya və rəqəmsal etimad mühitinin gücləndirilməsi kimi konkret addımları nəzərdə tutur [30].

Beləliklə, qeyd etmək olar ki, Azərbaycan Respublikasında rəqəmsal ticarət sahəsinin hüquqi tənzimlənməsi son illərdə nəzərəçarpacaq dərəcədə inkişaf etmiş və müasir rəqəmsal münasibətlərin əsas istiqamətlərini əhatə edən normativ baza formalaşdırılmışdır. Elektron ticarət, ödəniş sistemləri və fərdi məlumatların qorunması sahəsində qəbul olunmuş qanunvericilik aktları rəqəmsal iqtisadiyyatın hüquqi əsaslarını təmin etməkdədir. Mövcud çərçivə rəqəmsal mühitdə hüquqi münasibətlərin başlıca elementlərini tənzimləyir və hüquqi müəyyənlik baxımından mühüm rol oynayır. Bununla belə, texnoloji inkişafın dinamikası nəzərə alındıqda tənzimləyici çərçivənin mərhələli şəkildə təkmilləşdirilməsi və çevikləşdirilməsi gələcək üçün prioritet istiqamətlərdən biri kimi qiymətləndirilə bilər.

V. Nəticə

Elektron ticarətin adı nə qədər cəlbedici səslənsə də, kibertəhlükəsizlik təhdidləri ilə tez-tez üzləşir. Şirkətlər bu problemi həll etmək üçün davamlı olaraq çoxlu sərmayə qoysalar da, bu çıxış yolu hesab edilmir. Elektron ticarətə investisiya qoymaq və təhlükəsizliyini artırmaq rəqabət üstünlüyü əldə etmək və e-ticarət biznesinin uğuru üçün əhəmiyyətli dərəcədə vacibdir. Həm təşkilati, həm də müştəri ilə bağlı hər hansı nasazlıqdan əvvəl güclü monitorinq protokollarına əməl edilməlidir. Effektiv kibertəhlükəsizlik tədbirlərinin tətbiqi rəqəmsal ticarətin etibarlılığını artırmaqla yanaşı, iqtisadi sabitliyin və istifadəçi hüquqlarının qorunmasına da xidmət edir. Belə nəticəyə gəlirik ki, işçilər və istehlakçılar e-ticarət etmək üçün nə qədər təlim keçmiş və bacarıqlı olsalar və e-ticarət firması nə qədər kibertəhlükəsizlik protokolları və siyasətlərini həyata keçirsə belə, kibertəhlükəsizlik təhdidlərinin çağırışı biznesə zərər vermək üçün həmişə aktual problem olaraq qalacaqdır. Beynəlxalq təcrübə və qanunvericilik

bazalarının təhlili göstərir ki, ABŞ, Çin və Avropa İttifaqı rəqəmsal ticarət və kibertəhlükəsizlik sahəsində daha inkişaf etmiş və kompleks hüquqi mexanizmlərə malikdirlər. Azərbaycan qanunvericiliyi isə sürətlə inkişaf edir və rəqəmsal iqtisadiyyatın əsas komponentlərini əhatə edən normativ bazanı formalaşdırsa da, beynəlxalq standartlarla tam uyğunlaşma istiqamətində əlavə addımların atılması zəruridir.

ƏDƏBİYYAT (REFERENCES):

1. Al Naim, A.F., Ghouri, A.M. Exploring the Role of Cyber Security Measures (Encryption, Firewalls, and Authentication Protocols) in Preventing Cyber-Attacks on E-Commerce Platforms. International Journal of eBusiness and eGovernment Studies, 15(1), 2023, p. 444-469.
2. Araalan, Cemal. Teknik ve Hukuki Boyutlarıyla Elektronik Ödeme Sistemlerinde Siber Güvenlik, Seçkin Yayıncılık, 1. Baskı, Ankara, 2021. s. 288.
3. Alsayed, Alhuseen Omar / Bilgrami, Anwar, "E-Banking Security: Internet Hacking, Phishing Attacks, Analysisand Prevention of Fradulent Activities", International Journal of Emerging Technology and Advanced Engineering, C. 7, S. 1, 2017. p. 184.
4. Altinkaynak, Mustafa. Applied Cybersecurity and Hacking. Abakus Publishing, 5th ed., 2018, p. 288 (in Turkish / *Altınkaynak, Mustafa. Uygulamalı Siber Güvenlik ve Hacking, Abaküs Kitap, 5. Baskı, 2018. s. 288*).
5. Burke, Stephen. "How to prepare for the onslaught of phishing email attacks", Computer Fraud & Security, vol. 2021, Issue 5, p. 12-14.
6. Danish, Javeed and et. all., Man in the Middle Attacks: Analysis, Motivation and Prevention. VOL. 8, NO. 7, 2020, p. 52–58.
7. Dastres, R., Soori, M. Secure Socket Layer (SSL) in the Network and Web Security. World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering, Vol:14, No:10, 2020. p. 330-333.
8. Dülger, Murat Volkan. Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, 10. Baskı, 2023, s. 1008.
9. Elkamchouchi, Hassan M., An Improvement to the Set Protocol Based on Signcryption. International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 2, 2013. p. 1-13.
10. Eralp, Özgür. "İnternet Bankacılığı ve Kredi Kartı Dolandırıcılığının Teknik, Hukuki ve Cezai Boyutu, Eralp Kitap, Ankara, 2012, s. 71-96.
11. Ezenwe, Adaoma / FUREY, Eoghan / CURRAN, Kevin. "Mitigating Denial of Service Attacks with Load Balancing", Letterkenny Institute of Technology School of Computing, Journal of Robotics and Control, Vol 1 - 4, 2020, p. 129-135.
12. European Commission. (2016). Directive (EU) 2016/1148 (NIS Directive).

URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng (last access: 09.01.2025).

13. European Commission. (2022). Directive (EU) 2022/2555 (NIS2 Directive).
    URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (last access: 10.01.2025).
14. Greenleaf, G.California's CCPA as a Global Privacy Model. Privacy laws & Business International Report, (165), 2019. p. 1-4.
15. Global Risks Report 2024.
    URL: https://www.weforum.org/publications/global-risks-report-2024/ (last access: 09.01.2025).
16. Gómez, J.M., & Lichtenberg, J. Intrusion Detection Management System for eCommerce Security. Journal of Information Privacy and Security, 3(4), 2007. p. 19–31.
17. Gungor, Nevzat. Information Technologies and Cybersecurity in Internal Audit. 1st ed., Gazi Bookstore, Ankara, 2021, p. 139 (in Turkish / *Güngör, Nevzat, İç Denetimde Bilgi Teknolojileri ve Siber Güvenlik, 1. Baskı, Gazi Kitabevi, Ankara, 2021, s. 139*).
18. Harmening, T.J. Computer and Information Security Handbook (Third Edition), Chapter 58 - Virtual Private Networks. Morgan Kaufmann Publishers, Elsevier, 2017, p. 843-856.
19. Hogben, Giles. "Botnets: Measurement, Detection, Disinfection and Defence", ENISA's Emerging and Future Risk Programme, 2011. p. 138.
20. Law of the Republic of Azerbaijan on Electronic Commerce (in Azerbaijani / *"Elektron ticarət haqqında" Azərbaycan Respublikasının Qanunu*).
    URL: https://e-qanun.az/framework/10406 (last access: 08.01.2025).
21. Law of the Republic of Azerbaijan on Personal Data (in Azerbaijani / *"Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu*).
    URL: https://e-qanun.az/framework/19675 (last access: 10.01.2025).
22. Law of the Republic of Azerbaijan on Payment Services and Payment Systems (in Azerbaijani / *"Ödəniş xidmətləri və ödəniş sistemləri haqqında" Azərbaycan Respublikasının Qanunu*).
    URL: https://e-qanun.az/framework/54872 (last access: 09.01.2025).
23. Kemp, R. China's Data Security Law and its Global Impact. Journal of Data Protection & Privacy, 4(3), 2021, p. 210-226.
24. Keser, Berber Leyla/LOSTAR, Murat. Bilişimde Biyometrik Yöntemler, Yetkin Yayınları, 1. Baskı, Ankara, 2006, s. 132.
25. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, Barrett, M. (2018). URL: https://doi.org/10.6028/NIST.CSWP.04162018 / https://www.nist.gov/cyberframework (last access: 09.01.2025).

26. Nezhad, S.M.T., Nazari, M., Gharavol, E.A.: A novel DoS and DDoS attacks detection algorithm using arima time series model and chaotic system in computer networks. IEEE Commun. Lett. 20(4), 2016, p. 700–703.
27. NPC. Cybersecurity Law of the People's Republic of China. National Peoples's Congress. (2016).
URL: https://shorturl.at/ntwDp (last access: 08.01.2025).
28. OECD, Computer Viruses and Other Malicious Software: A Threat to the Internet Economy, Paris: OECD Publishing, 2009, s. 21.
29. Özmen, Şule, Ağ Ekonomisinde Yeni Ticaret Yolu: E-Ticaret, İstanbul Bilgi Üniversitesi Yayınları, 5. Baskı, İstanbul, 2013. p. 544.
30. Order of the President of the Republic of Azerbaijan on approval of the "Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023-2027". (in Azerbaijani / *Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası*).
URL: https://e-qanun.az/framework/55045 (last access: 11.01.2025).
31. Rehida, Pavlo/Markowsky, George/Sachenko, Anatoliy/Savenko, Oleg, "State-based Sandbox Tool for Distributed Malware Detection with Avoid Techniques". The 13th IEEE International Conference on Dependable Systems, Services and Technologies, Greece, 2023, p. 553-558.
32. Solove, D.J., and Hartzog, W. The FTC and the New Common Law of Privacy. Columbia Law Review 114(3), 2008, p. 583-676.
33. Statista, "Annual Number of Malware Attacks Worldwide from 2015 To 2023".
URL: https://shorturl.at/HUTno (last access: 09.01.2025).
34. Taner, Cemal. Herkes İçin Siber Güvenlik, Abaküs, 1. Baskı, İstanbul, 2019, s. 176.
35. Tikkinen-Piri, C., Rohunen, A., & Markkula, J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 2018, p. 134–153.
36. U.S. Congress. Cybersecurity Information Sharing Act (CISA). Division N of Public Law, 114-113.
URL: https://shorturl.at/TVQk0 (last access: 10.01.2025).
37. USOM, Siber Güvenliğe İlişkin Temel Bilgiler, USOM, 2014, s. 12.
38. Voigt, P., & Von dem Bussche, A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer. 2017, p. 175.
39. Yuan, X., Li, C., Li, X.: DeepDefense: identifying DDoS attack via deep learning. IEEE International Conference on Smart Computing (SMARTCOMP), 2017, p. 1–8.

40. Zhou, W., and Arner, D. PIPL vs GDPR: Divergences and Convergences. Asian Journal of Law and Technology, 11(1), 2022, p. 34-49.
41. ZHU, Y. et al., "Improving E-Commerce Order Fulfillment for Peak Times via Incorporating Fulfillment Network Load Balancing. ISEC, IBM T.J. Watson Research Center, 2017, p. 1802-1809.

Analysis of cyberattacks in electronic commerce: legal approaches of the Republic of Azerbaijan and other countries

KAMRAN KHALILOV*

Abstract

In the reality of the 21st century, the rapid development of information technologies has stimulated the digitalization processes in the global economy and has led to fundamental changes in the trade sector. As a result of the rise of e-commerce, the collection, storage and processing of personal data in the electronic environment has become widespread. While this process has created convenience and accessibility for consumers on the one hand, it has also led to the emergence of new and complex risks in the field of personal data security on the other. In particular, the large-scale processing of personal data has created favorable targets for cybercriminals and has led to e-commerce platforms being faced with various types of cyber threats. The study conducted in this context identifies the main risk factors and common cyberattack methods that threaten the security of personal data in the e-commerce sector. The article examines the impact of methods such as social engineering, phishing, DDoS attacks and malware on e-commerce and presents preventive technological and legal measures that can be applied against these risks. The study also assessed the legal consequences of data breaches, companies' obligations for accountability and data protection, and reputational and economic losses arising from the impact of breaches. The study analyzed the regulatory frameworks of various countries, in particular the General Data Protection Regulation (GDPR) of the European Union, the California Consumer Data Protection Act (CCPA) of the United States, and the Law of the Republic of Azerbaijan "On Personal Data" based on both doctrinal and comparative law methodologies. As a result of the comparison, significant differences were identified between these regulatory acts in terms of data processing principles, data breach notification regimes, individual consent, legal liability, and sanction mechanisms. The study focused on the application of a risk-based approach and the possibilities of integrating

* PhD Student in Law / Department of Criminal Procedure, Baku State University / Lecturer at the Academy of the State Security Service of the Republic of Azerbaijan named after Heydar Aliyev / email: kamran.khalilov.isa@bsu.edu.az

this model into both information security policies and national legal regulations. The scientific novelty of the article lies in the fact that it presents a complex and multidisciplinary analysis by combining legal and technical approaches. In conclusion, this study proposes practical and theoretical recommendations for the formation of an effective model in terms of regulatory compliance, legal accountability, and technical resilience, using national and international practices for ensuring cybersecurity in the e-commerce sector.

Keywords: *cyberattack, e-commerce, malware, legislative framework, security, prevention, defense, strategy, legal regulation.*

Анализ кибератак в электронной коммерции: правовые подходы Азербайджанской Республики и других стран

КАМРАН ХАЛИЛОВ[**]

Резюме

В реалиях XXI века стремительное развитие информационных технологий стимулировало процессы цифровизации мировой экономики и привело к фундаментальным изменениям в сфере торговли. В результате развития электронной коммерции сбор, хранение и обработка персональных данных в электронной среде получили широкое распространение. С одной стороны, этот процесс создал удобство и доступность для потребителей, с другой стороны, он также привел к появлению новых и сложных рисков в области безопасности персональных данных. В частности, масштабная обработка персональных данных создала благоприятные мишени для киберпреступников и привела к тому, что платформы электронной коммерции сталкиваются с различными видами киберугроз. Проведенное в этом контексте исследование выявляет основные факторы риска и распространенные методы кибератак, угрожающие безопасности персональных данных в секторе электронной коммерции. В статье рассматривается влияние таких методов, как социальная инженерия, фишинг, DDoS-атаки и вредоносное программное обеспечение, на электронную коммерцию, а также представлены превентивные технологические и правовые меры, которые могут быть применены для борьбы с этими рисками. В исследовании также оценивались правовые последствия утечек данных, обязательства компаний по подотчётности и защите данных, а также репутационные и экономические потери, возникающие в результате утечек. В исследовании

[**] Докторант / кафедра уголовного процесса Бакинского государственного университета / Преподаватель Службы Академии Государственной Безопасности Азербайджанской Республики имени Гейдара Алиева / email: kamran.khalilov.isa@bsu.edu.az

анализировалась нормативная база различных стран, в частности, Общий регламент по защите данных (GDPR) Европейского Союза, Закон о защите данных потребителей штата Калифорния (CCPA) США и Закон Азербайджанской Республики «О персональных данных», на основе как доктринальных, так и сравнительно-правовых методологий. В результате сравнения были выявлены существенные различия между этими нормативными актами в части принципов обработки данных, режимов уведомления об утечках данных, индивидуального согласия, юридической ответственности и механизмов санкций. Исследование было сосредоточено на применении риск-ориентированного подхода и возможностях интеграции этой модели как в политику информационной безопасности, так и в национальные правовые нормы. Научная новизна статьи заключается в том, что она представляет собой комплексный и междисциплинарный анализ, сочетающий юридические и технические подходы. В заключение исследования предлагаются практические и теоретические рекомендации по формированию эффективной модели с точки зрения соблюдения нормативных требований, правовой ответственности и технической устойчивости с использованием национального и международного опыта обеспечения кибербезопасности в секторе электронной коммерции.

Ключевые слова: *кибератака, электронная коммерция, вредоносное ПО, законодательная база, безопасность, профилактика, защита, стратегия, правовое регулирование.*

Redaksiyaya daxil olma tarixi: 17.01.2025
Çapa qəbul: 11.09.2025