UDC 542.23
DOI 10.52171/herald.303

Analysis and Assessment of Security in Cyber-Physical Systems

P.A. Abbasova
Azerbaijan Technological University (Ganja, Azerbaijan)

For correspondence:
Parvin Abbasova / e-mail: p.abbasova@atu.edu.az

Abstract

With the digitalization of the world, cyber attacks have entered our lives, initially possessing a simple and easily understandable structure. However, today they have become increasingly complex and difficult to investigate. To address this problem, the collection of intelligence data related to attacks before they occur, and their detection after they happen, have become two essential components of modern cybersecurity. In particular, the successful integration of large-scale network infrastructures into the field of cybersecurity in recent times has made it necessary to utilize these technologies both in cyber threat intelligence and attack detection systems. This study explores cyber threat intelligence, attack detection systems, and large-scale network technologies, reviews the work focused on cyber threat intelligence and attack detection systems that utilize large network technologies, and provides various evaluations.

Keywords: cyber-physical system, IoT, information security, cybersecurity, cyber death, risk.

Submitted *14 April 2025*
Published *22 September 2025*

For citation:
P.A. Abbasova
[Analysis and Assessment of Security in Cyber-Physical Systems]
Herald of the Azerbaijan Engineering Academy, 2025, vol. 17 (3), pp. 111-118

Kiberfiziki sistemlerdə təhlükəsizliyin analizi və qiymətləndirilməsi

P.Ə. Abbasova

Azərbaycan Texnologiya Universiteti (Gəncə, Azərbaycan)

Xülasə

Rəqəmsallaşan dünya ilə bərabər həyatımıza daxil olan kiber hücumlar əvvəllər sadə və aydınlaşdırılması asan struktur idi. Lakin bugün artiq qarışıq bir struktura sahib və tədqiq edilməsi çətin hal almışdır. Bu problemi aradan qaldırmaq məqsədilə hücumların gerçəkləşmədən əvvəl onlara aid kəşfiyyat məlumatların toplanması, həyata keçdikdən sonra isə tapılması günümüzün ayrılmaz iki əsas ünsürü olmuşdur. Xüsusilə son zamanlarda böyük şəbəkə avadanlıqlarınında kiber təhlükəsizlik sahəsinə uğurla tətbiqi, istər kiber təhdid kəşfiyyatı istərsə də hücum təhlükəsi sistemlərində bu texnologiyalardan faydalanmağı məcbur etmişdir. Bu işdə kiber təhdid kəşfiyyatı, hücum təhlükəsi sistemləri və böyük şəbəkə texnologiyaları açıqlanmış, böyük şəbəkə texnologiyalarından faydalanan kiber təhdid kəşfiyyatı və hücum təhlükəsi sistemlərinə yönəlmiş işlər nəzərdən keçirilmiş və müxtəlif qiymətləndirilmələr edilmişdir.

Açar sözlər: kiberfiziki sistem, əşyaların interneti (IoT), informasiya təhlükəsizliyi, kibertəhlükəsizlik, kiber ölüm, risk

---

Анализ и оценка безопасности в киберфизических системах

П.А. Аббасова

Азербайджанский технологический университет (Гянджа, Азербайджан)

Аннотация

С развитием цифрового мира кибератаки вошли в нашу жизнь, изначально имея простую и легко объяснимую структуру. Однако сегодня они приобрели сложный характер, и их анализ стал затруднительным. С целью устранения данной проблемы сбор разведывательной информации о киберугрозах до их реализации, а также их обнаружение после атаки стали двумя неотъемлемыми элементами современной кибербезопасности. Успешное применение крупномасштабного сетевого оборудования в области кибербезопасности, особенно в последнее время, сделало использование этих технологий необходимым как в системах киберугрозной разведки, так и в системах обнаружения атак. В данной работе рассматриваются киберугрозная разведка, системы обнаружения атак и крупномасштабные сетевые технологии, а также анализируются исследования, направленные на применение таких технологий в системах кибербезопасности, и представлены различные оценки.

Ключевые слова: киберфизическая система, интернет вещей (IoT), информационная безопасность, кибербезопасность, киберсмерть, риск.

Giriş

İnformasiya və kommunikasiya texnologiyalarının sürətlə inkişaf etdiyi dövrdə sosial strukturların və aktorların hər bir səviyyəsi mürəkkəb və qeyri-müəyyənliklərlə dolu bir mühitdə yaşamalı olur. Yaşadığımız əsrin postmodern şəraitində çaşqınlıq və qaranlıqla dolu dünyanın mərkəzində şübhəsiz ki, təhlükəsizlik anlayışı dayanır. Kiberməkan adlanan və informasiya-kommunikasiya texnologiyalarının yaratdığı, kompüter sistemlərini, onlayn kommunikasiya şəbəkələrini və idarəetmə proseslərini özündə birləşdirən bu nəhəng dünya qlobal miqyasda sosial, iqtisadi, siyasi və mədəni inteqrasiyanın tərkib hissəsi kimi sürətlə inkişaf edir. Belə inteqrasiyanın əsasını bilik təşkil edir. İnformasiya cari əsrin ən mühüm istehsal və istehlak məhsuludur. Biliyə əsaslanmayan hər hansı məhsul və ya xidmət istənilən keyfiyyət və standart sayılmır [1].

Müasir kiber dünyasının ən əsas elementi internet bazasıdır. Hal-hazırda istifadə olunan bütün kompüterlər, elektrik xətləri, radiolar, peyk sistemləri, hər cür elektrik və elektromaqnit cihazları, mobil telefonlar, peyklər, robot sistemlər, bütün insanlı və ya pilotsuz hava, quru və dəniz nəqliyyat vasitələri internet bazasında kodlanmış proqram sistemləri sayəsində işləyir. Bütün bu alətlər və avadanlıqlar həm də kiberməkan dünyasının mühüm elementləri hesab olunur. Bu vasitələrin və bütövlükdə internet bazasının təhlükəsizliyi çox vacibdir. Son illərdə mütəşəkkil cinayətkarlıq və terror təşkilatları öz fəaliyyətlərini planlaşdırmaq, təlimlər keçirmək, informasiya və təbliğat texnikalarını paylaşmaq kimi diqqətlərini kiberməkana yönəltmiş, məqsədlərinə çatmaq üçün informasiya-kommunikasiya texnologiyalarından istifadə etmişlər.

Kibertəhlükəsizlik və müdafiə fəaliyyətləri aktivləşdirdikləri hücum və təhdidlərə görə fərdlər, qurumlar, təşkilatlar və dövlətlər səviyyəsində əhəmiyyətini artırmışdır. Kiber dünyanın ən mühüm açarı olan təhlükəsizlik şəbəkəsi, müasir həyatın adi təhlükəsizlik anlayışları ilə inteqrasiya olunaraq kibertəhlükəsizlik anlayışı adlandırılmağa başlayıb. Ədəbiyyatda kibertəhlükəsizliklə bağlı bir çox təriflər verilməyə çalışılsa da, artıq bütün sətirləri ilə ortaya çıxan kibertəhlükəsizlik anlayışından danışmaq mümkün deyil [2]. Bu vəziyyətin əsas səbəbi kibertəhlükəsizlik anlayışının ölçü və sərhədlərinin çəkilə bilməməsidir. Əslində, informasiya-kommunikasiya texnologiyalarının qlobal internet şəbəkəsi ilə inteqrasiyası və müasir həyatın sahələrinə daxil olması kibertəhlükəsizlik konsepsiyasının çərçivəsini əngəlləyir. Bununla belə kibertəhlükəsizlik anlayışı informasiya-kommunikasiya texnologiyalarının çox sürətlə inkişaf etdiyi bu gün ayrı-ayrı şəxslərin, qurumların, beynəlxalq təşkilatların və dövlətlərin ən mühüm gündəm məsələlərindən birinə çevrilib. Bu gün əhəmiyyəti danılmaz hala gələn kibertəhlükəsizlik anlayışı qlobal postmodern sivilizasiya prosesinin daimi mövzusu olacaqdır. Kibertəhlükəsizlik sahəsində hər gün bir çox təhlükələr meydana çıxsa da, bu təhlükələri kateqoriyalara bölmək mümkündür.

İşin məqsədi

Kiberfiziki sistemlərdə təhlükəsizliyin qiymətləndirilməsi, kiber təhlükəsizlik və informasiya təhlükəsizliyi arasındakı fərqlərin aydınlaşdırılması, habelə KFS-in təhlükəsizlik təhdidləri ilə mübarizənin müasir yanaşmalarını təqdim etməkdir. Eyni zamanda, kiber öldürmə zəncirinin və hücumların qarşısını alma üsullarının tədqiqi, bu sahədə mövcud məhdudiyyətlər, problemlər və gələcək tendensiyalar da müzakirə ediləcəkdir.

Məsələnin qoyuluşu

Kiberfiziki sistemlərin təhlükəsizliyi və bu sahədəki mövcud təhdidlərə qarşı mübarizə üsullarını araşdırır. Həmçinin, kiber təhlükəsizlik və informasiya təhlükəsizliyi arasındakı fərqlər, bu sahədəki məhdudiyyətlər və gələcəkdə tətbiq olunacaq yeni yanaşmalar müzakirə ediləcəkdir.

Məsələnin həlli

Kiberfiziki sistemlər (KFS) sensorlar və aktuatorların köməyi ilə fiziki dünyanı virtual hesablama dünyası ilə əlaqələndirir. Müxtəlif tərkib komponentlərindən ibarət olan KFS-lər əməkdaşlıqda qlobal davranışlar yaradır. Bu komponentlərə real dünya ilə qarşılıqlı əlaqə yaratmaq üçün proqram sistemləri, kommunikasiya texnologiyaları, sensorlar/aktuatorlar, o cümlədən tez-tez quraşdırılmış texnologiyalar daxildir. Bu iki dünyanı birləşdirən Kiber-Fiziki Sistemlər iki mühüm elementdən ibarətdir: internet üzərindən və təyin edilmiş internet ünvanı ilə bir-biri ilə əlaqə saxlayan obyektlər və sistemlər tərəfindən yaradılmış şəbəkədən. Bu, kompüter mühitində real dünya obyektlərinin və davranışlarının simulyasiyası ilə yaradılmış virtual mühitdir.

Kiber-Fiziki Sistemlər təkcə istehsalda deyil, həm də bir çox yerlərdə mühüm rol oynayır. Onlardan bəzilərini belə sıralamaq olar: Fiziki və təşkilati iş proseslərinə nəzarət edir; Əhəmiyyətli istifadəçi əlaqəsini ehtiva edir; Real vaxtda konfiqurasiya, yerləşdirmə və ya təyinatla mühitdəki reaktiv dəyişikliklərə uyğunlaşır və təkamül edir; Öz performansını daim izləyir və optimallaşdırır; Yüksək dərəcədə etibarlılıq tələb edir; Müxtəlif texniki fənlərin və müxtəlif tətbiq sahələrinin inteqrasiyasını tələb edir.

Kiber təhlükəsizlik və informasiya təhlükəsizliyi arasındakı fərq

Kompüter şəbəkələrindən istifadənin getdikcə artması və onların həyatımızın bir çox sahələrinə daxil edilməsi, informasiya təhlükəsizliyinin təmin edilməsi problemini özü ilə gətirdi [3]. Bu halda kibertəhlükəsizliyin tərifi ilə birlikdə cavablandırılması lazım olan bir sual da, "İnformasiya Təhlükəsizliyi"-ni "Kibertəhlükəsizlik"-dən fərqli və ortaq cəhətlərinin nə olduğudur.

İnformasiya təhlükəsizliyi - təqdim olunan xidmətlərin, sistemlərin və məlumatların qorunmasını təmin edir.

Kibertəhlükəsizlik - kompüterlərin, məlumatların və şəbəkələrin icazəsiz rəqəmsallaşdırılmasıdır.

Bu, müxtəlif üsul və texnologiyalardan istifadə etməklə hücumların, girişin və ya məhv edilmənin qorunmasıdır.

KFS-in təhlükəsizlik təhdidləri

Təhlükəsizliyin mahiyyəti hər hansı məlumatdır. Məlumat yoxdursa, təhlükəsizlik də yoxdur. Təhlükəsizliyin təmin edilməsi üçün bütün gizli, açıq, texniki, ictimai məlumatlandırma fəaliyyətləri kəşfiyyat adlanır. İnformasiya prosesləri kiber kəşfiyyat fəaliyyəti olaraq ortaya çıxdı. Kibertəhlükə kiber kəşfiyyatın alt hissəsi kimi xüsusi təhsili olan, xüsusi texnologiya və məlumatlardan istifadə edən, elmə əsaslanan bir fəndir. Buna görə kiber kəşfiyyatda texnologiyadan istifadə edirik və buna görə də kiber təhlükə kəşfiyyatı istifadəsi olduqca vacibdir. İstifadə edilə bilən bu texnologiyalardan biri də blok zənciri texnologiyasıdır. Blockchain (blok zənciri) texnologiyası prosesləri pozmaq potensialına malikdir və istifadə etdiyi kriptoqrafik protokollar sayəsində rədd edilməməsi və dəyişməzlik xüsusiyyətləri ilə təhlükəsizdir. Məlumatların işlənməsinin

və məlumat mənbəyinin qorunmasının daha yüksək səviyyəsinə zəmanət verir.

Kiber təhlükəsizliyin mübarizə apardığı təhdidləri beş başlıq altında nəzərdən keçirmək olar: Haktivizm; Kibercinayətkarlıq; KiberSabotaj; Kiberterrorizm; Kibermüharibə.

Kiber öldürmə zəncirinin və hücumun qarşısının alınması üsullarının tədqiqi

Kiber ölüm zənciri Amerikanın qlobal aerokosmik, müdafiə, təhlükəsizlik və qabaqcıl texnologiya şirkəti olan Lockheed-in nəticəsidir. Martin tərəfindən hazırlanmışdır. Kiber ölüm zənciri, kəşfiyyat və kompüter şəbəkələrinin müdafiəsi üçün fokuslanmış təhlükə modelidir [4].

"Ölüm Zənciri"nə görə, hədəflənmiş kiberhücum 7 mərhələdə baş verir: 1.Kəşfiyyat (**Reconnaissance**); 2. Silahlanma (Weaponization); 3. Çatdırılma (Delivery); 4. İstismar (Exploitation); 5. Quraşdırma (Installation); 6. Komanda və Nəzarət (Command & Control, C2); 7. Məqsədlər üzrə Fəaliyyətlər (Actions On Objectives).

Kəşfiyyat (Reconnaissance)

Bu, hücumçunun hədəf sistem haqqında məlumat toplama mərhələsidir. Bu mərhələnin məqsədi sistemə infiltrasiya üsullarını aşkar etməkdir. Bu mərhələdə hədəf seçimi, təşkilatın ətraflı tədqiqi, hədəfin texnologiya seçimləri, sosial şəbəkə fəaliyyətləri araşdırılır.Eyni zamanda təcavüzkarlar hədəflərinə qarşı hansı hücum üsullarının daha yaxşı olduğunu müəyyənləşdirir və təsirli olub-olmayacağını öyrənməyə çalışır.

Silahlanma (Weaponization)

Kəşfetmə mərhələsində hədəf sistemə giriş nöqtəsini təyin edən təcavüzkar bu giriş nöqtəsində hansı hücum vektorundan istifadə edəcəyinə qərar verir. Eyni zamanda istifadə ediləcək zərərli proqram da bu mərhələdə yaradılır. Bu mərhələdə müdafiəçilər silahı olduğu kimi aşkar edə bilməsələr də, zərərli proqram əsərlərini təhlil edərək nəticə çıxara bilirlər. Bu analizlər adətən ən davamlı müdafiədir.

Çatdırılma (Delivery)

Zərərli proqramın hədəf sistemə göndərildiyi mərhələ. Bu mərhələdə təcavüzkar lazımi anonimliyə nail ola bilmədiyi müddətcə izlər buraxa bilər. Bu səbəblə təhlükəsizliyin ən zəif halqası olan insan nəzərə alınır və e-poçt və ya usb kimi zərərli vasitələr idarə edilir.

İstismar (Exploitation)

Təcavüzkarın silahlanma mərhələsində yaradılmış hücum vektorundan istifadə edərək hədəf sistemdəki təhlükəsizlik zəifliyindən istifadə etdiyi mərhələdir. Burada məqsəd zərərli proqramın sistemdə işləməsini təmin etməkdir [5].

Yükləmə mərhələsi ilə kompüterə endirilən fayl işə salındıqda sistemdə zəiflik yaranır. Onu istismar etməklə yükləmə mərhələsi açılacaq .

Quraşdırma (Installation)

Zərərli proqramın hədəf sistemdə qalma müddətini artırmaq üçün proqram təminatının sistemə quraşdırıldığı mərhələ. Faylların və metadataların silinməsi, möhürlər və kritik məlumatları dəyişdirə bilər ki, sanki giriş heç vaxt verilməyib.

Komanda və Nəzarət (Command & Control, C2)

Bu mərhələdə hədəf sistem tutulur. Təcavüzkar indi şəbəkənin aşağı hissəsində zərərli kodu tam manipulyasiya edə bilər. O, irəliləyə məlumat sızdıra və məhvetmə və ya xidmətdən imtina əməliyyatları həyata keçirə bilər.mBu mərhələdə quraşdırılmış hücum alətlərini idarə etmək üçün C2 kanalı qurulur.

Məqsədlər üzrə Fəaliyyətlər (Actions On Objectives)

Hədəf sistemini ələ keçirən hücumçu bu mərhələ ilə məqsədinə çatmaq üçün müxtəlif hərəkətlər edir. Bu hərəkətlərə misal olaraq məlumatların çıxarılması, silinməsi və ya başqa sistemə hücumu ola bilər.

Kiberfiziki sistemlər – fon

Bu bölmədə biz Kiberfiziki sistemlər arxitekturasını, onun əsas təbəqələrini və komponentlərini, həmçinin əsas kiberfiziki sistemlər modellərini təqdim edirik [6]. Kiberfiziki sistemlər səviyyələri kiberfiziki sistemlərin arxitekturası üç əsas təbəqədən, aşkarlama qatından, ötürücü təbəqədən və tətbiq səviyyəsindən ibarətdir.

Aşkarlama qatı: tanınma və ya aşkarlama təbəqəsi kimi də tanınır. Buraya sensorlar, aktuatorlar, kollektorlar, həmçinin radiotezliklərin identifikasiyası etiketləri, qlobal mövqeləşdirmə sistemləri və müxtəlif digər cihazlar kimi avadanlıqlar daxildir. Bu cihazlar fiziki dünyanı izləmək və şərh etmək üçün real vaxt rejimində məlumat toplayır.

Ötürücü təbəqə: Həmçinin nəqliyyat qatı və ya şəbəkə qatı kimi tanınır və ikinci kiberfiziki sistem qatıdır. Bu təbəqə qavrayış və tətbiq səviyyələri arasında məlumat mübadiləsini və emalnı edir.

Tətbiq səviyyəsi: Üçüncü və ən interaktiv təbəqədir. O, məlumat ötürmə səviyyəsindən alınan məlumatları emal edir, sensorlar və aktuatorlar da daxil olmaqla fiziki bölmələr tərəfindən yerinə yetirilən əmrlər verir. Bu, ümumiləşdirilmiş məlumatlar əsasında mürəkkəb qərar qəbul etmə alqoritmlərinin tətbiqi ilə həyata keçirilir.

Kiberfiziki sistemlərdə məhdudiyyətlər, problemlər və gələcək tendensiyalar

Kiberfiziki sistemlər fiziki giriş və çıxışla qarşılıqlı əlaqədə olan daxili sistemlər şəbəkəsi kimi müəyyən edilir. Başqa sözlə, kiberfiziki sistemlər real IoT ilə əlaqəli obyektləri və prosesləri izləmək və emal etmək imkanı ilə bir-biri ilə əlaqəli bir neçə sistemin birləşməsindən ibarətdir. Kiberfiziki sistemlər üç əsas mərkəzi komponentdən ibarətdir: sensorlar, kollektorlar və aktuatorlar.

Problemin formalaşdırılması

Çoxsaylı üstünlüklərinə baxmayaraq, kiberfiziki sistemlər müxtəlif kiber və fiziki təhlükəsizlik təhdidlərinə, hücumlara və çağırışlara qarşı həssasdır. Bunun səbəbi onların heterojen təbiəti, özəl və həssas məlumatlara etibarı və geniş miqyaslı paylanmasıdır. Bundan əlavə, davamlı proqram təminatı, tətbiq və əməliyyat sistemi yeniləmələri ilə təhlükəsizlik zəifliklərı minimuma endirilməlidir.

Motivasiya

Kiberfiziki sistemlərin təhlükəsizliyi sistemləri kritik infrastrukturlara (ağıllı şəbəkə, sənaye, təchizat zənciri, səhiyyə, hərbi, kənd təsərrüfatı və s.) inteqrasiya olunub. Bu, onları iqtisadi, cinayət, hərbi, casusluq, siyasi və müxtəlif məqsədlər üçün təhlükəsizlik hücumları üçün cəlbedici hədəfə çevirir.

Töhfələr

Bu araşdırmada biz kiberfiziki sistemlərin müxtəlif kiber-fiziki təhlükəsizlik aspektlərinin hərtərəfli nəzərdən keçirilməsini və təhlilini təqdim edirik [7].

Töhfələrə aşağıdakılar daxildir: Ümumi məlumat; Kiber-Fiziki Hücumlar; Riskin qiymətləndirilməsi; Təhlükəsizlik tədbirləri; Məhkəmə; Dərslər; Təkliflər.

Kiber təhlükəsizlik auditində Məqsədlər

Hər bir auditdə olduğu kimi, kibertəhlükəsizlik yoxlamalarınında məqsədi olmalıdır. Kibertəhlükəsizlik auditinin məqsədi rəhbərliyə kibertəhlükəsizlik prosesləri, siyasətlər, prosedurlar, idarəetmə və digər nəzarət vasitə-

lərinin effektivliyini qiymətləndirməyə imkan yaratmaqdır [8].

Rəhbərliyə sistemli,elmi təminat və məsləhət xidmətləri göstərməkdir.

Auditin məqsədləri

Audit məqsədləri müəyyən edilə bilər. Bununla belə kibertəhlükəsizliklə bağlı məqsədlər aşağıdakı kimi məhdudlaşdırıla bilər:

- ✓ Kibertəhlükəsizlik siyasəti və prosedurları və onların işinin səmərəliliyinin qiymətləndirilməsi ilə rəhbərliyə etibarlılıqla təmin etmək;
- ✓ Təhlükəsizlik nəzarətindəki zəifliklər səbəbindən korporativ məlumatların etibarlılığına, dəqiqliyinə və təhlükəsizliyinə təsir etməklə idarəetməyə rəhbərlik etmək;
- ✓ Cavab və bərpa proqramlarının effektivliyini qiymətləndirərək institusional yanaşmaların daxililəşdirilməsinə kömək etmək.

Biznesə təsir və risklərin qiymətləndirilməsi

Kiber insident maliyyə, əməliyyat, hüquqi və reputasiyaya təsir göstərə bilər. Təşkilatın kritik infrastrukturda rolu vebsaytın potensial təsirini də artıra bilər [9]. Kiberhücumun nəticələri baxımından nəzərə alına biləcək neqativlərə aşağıdakılar misal ola bilər:

- ✓ Əqli mülkiyyət və ya ticarət sirrinin itirilməsi;
- ✓ Kibertəhlükəsizliyə nəzarəti azaltmaq və təkmilləşdirmək üçün texnologiyanın inkişaf xərcləri;
- ✓ Vaxt və səmərəlilik itkisi.

Buna görə də kibertəhlükəsizlik auditində kiber pozuntuların iş proseslərinə təsirləri çərçivəsində riskin qiymətləndirilməsi böyük əhəmiyyət kəsb edir.

Nəticə

Məqalədə kiberfiziki sistemlərin təhlükəsizliyi və bu sahədəki mövcud təhdidlərə qarşı tətbiq olunan müasir üsulların təhlilini təqdim edir. Kiber təhlükəsizlik və informasiya təhlükəsizliyi arasındakı fərqlər aydınlaşdırılmış və kiber öldürmə zəncirinin qarşısını almaq üçün effektiv strategiyalar təqdim edilmişdir. Həmçinin, kiberfiziki sistemlərdəki məhdudiyyətlər və problemlər üzərində dayanılaraq, gələcəkdə tətbiq ediləcək yeni yanaşmalar müzakirə edilmişdir. Kiber təhlükəsizlik auditi ilə bağlı məqsədlər müəyyən edilərək, bu sahədə daha da inkişaf edilməsi üçün təkliflər irəli sürülmüşdür.

Maraqlar münaqişəsi

Müəllif bu məqalədə araşdırılması tələb olunan maraqlar münaqişəsinin olmadığını qeyd edir.

REFERENCES

1. **Lynn T.** (2020). Cyber-security incidents and audit quality. European Accounting Review, 1-28.
2. **Morgan S.** 2017 Cybercrime Report", Cybersecurity Ventures, Herjavec Group, pp. 1-24, 2017.
3. **Al-Otaibi A.F., Alsuwat E.S.** A Study On Social Engineering Attacks: Phishing Attack, International Journal of Recent Advances in Multidisciplinary Research, 6374-6380, 2020.

4. **Garba F.A.** The anatomy of a cyber attack: dissecting the cyber kill chain (ckc), Scientific and Practical Cyber Security Journal, 2019.
5. **Yadav T., Mallari R.A.** Technical aspects of the cyber kill chain, In International Symposium on Security in Computing and Communication, 438-452, 2016.
6. **Abbasova P.Ə.** Kiberfiziki sistemlərdə Big Data analizi // Azərbaycan Mühəndislik Akademiyasının Xəbərləri, 2024, cild 16 (3), s. 81-86.
7. **Mahmoud R., Yousuf T., Aloul F., Zualkernan I**. 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) IEEE; 2015. Internet of things (IoT) security: current status, challenges and prospective measures; pp. 336–341.
8. **Faruque A., Abdullah M., Chhetri S.R., Canedo A., Wan J.** Acoustic side-channel attacks on additive manufacturing systems. In Proceedings of the 7th International Conference on Cyber-Physical Systems, page 19. IEEE Press, 2016.
9. **Dolgui A., Ivanov D., Sethi S.P., Sokolov B**. (2019). Scheduling in production, supply chain and Industry 4.0 systems by optimal control. International Journal of Production Research, 57(2), pp. 411-432.