# Dövlətin Kibersuverenliyinin Təmin Edilməsi üçün Milli Proqram Mühəndisliyinin Formalaşması Problemləri

Tamilla Bayramova
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
*tamilla@iit.science.az*

***Xülasə*— Tədqiqat işi müasir geosiyasi çağırışlar fonunda milli proqram mühəndisliyinin kibersuverenliyin və dövlətin rəqəmsal müstəqilliyinin təmin edilməsindəki rolunun təhlilinə həsr olunmuşdur. İşdə xarici proqram sistemlərindən asılılığın milli təhlükəsizlik üçün yaratdığı risklər, o cümlədən, kritik infrastrukturun həssaslığı və rəqəmsal aktivlər üzərində nəzarətin itirilməsi məsələləri araşdırılır. Milli texnoloji platformaların, milli rəqəmsal ekosistemin və yüksəkixtisaslı kadr potensialının formalaşdırılması kibersuverenliyin fundamental şərtlərindən biri kimi əsaslandırılır. İşdə milli proqram mühəndisliyinin inkişafını stimullaşdıran dövlət dəstəyi mexanizmləri, təhsil bazasının modernləşdirilməsi və proqram təminatının həyat dövründə kibertəhlükəsizlik prinsiplərinin inteqrasiyası üzrə tövsiyələr irəli sürülür.**

***Açar sözlər*— *kibertəhlükəsizlik; proqram mühəndisliyi; rəqəmsal suverenlik; kritik infrastruktur; təchizat zəncirinin təhlükəsizliyi; asılılıqların idarə edilməsi.***

## I. GİRİŞ

Müasir geosiyasi şəraitdə rəqəmsal texnologiyalar üzərində nəzarət dövlətlərin öz milli maraqlarını qlobal müstəvidə təşviq etmək və digər subyektlərə təsir göstərmək üçün istifadə etdiyi fundamental strateji alətə çevrilmişdir. Xarici mənşəli proqram sistemlərindən birtərəfli asılılıq, dövlətin suverenliyinə və milli təhlükəsizliyinə birbaşa təhdid yaradan həm siyasi, həm də iqtisadi təzyiq vasitəsi kimi çıxış edir. Bu baxımdan, milli proqram mühəndisliyi dövlətin rəqəmsal sahədə texnoloji müstəqilliyini təmin etməyə yönəlmiş, yerli intellektual resurslara əsaslanan proqram məhsullarının yaradılması üçün kompleks strateji yanaşmadır.

Milli proqram mühəndisliyi (PM) konsepti yalnız proqram təminatının yazılması ilə məhdudlaşmır; o, dövlətin öz standartlarının, milli platformalarının və rəqəmsal ekosistemlərinin işlənib hazırlanmasını ehtiva edir. Bu yanaşma milli informasiya infrastrukturunun fəaliyyəti üçün kənar müdaxilələrdən qorunan, dayanıqlı və şəffaf bir baza formalaşdırır. Cəmiyyətin bütün sahələrinin sürətlə rəqəmsallaşması şəraitində, milli PM dövlət siyasətinin mərkəzi elementinə çevrilərək, kritik rəqəmsal aktivlər üzərində tam nəzarətin bərqərar olmasına xidmət edir. Bu, qlobal rəqabətdə ölkənin kiberməkandakı mövqelərini möhkəmləndirməklə yanaşı, innovasiyaları stimullaşdırır və rəqabətqabiliyyətli yerli İT sənayesinin formalaşması üçün fundamental zəmin yaradır.

Azərbaycanın 2023-2027-ci illər üzrə İnformasiya Təhlükəsizliyi Strategiyası da məhz bu zərurətdən irəli gələrək, informasiya mühafizəsində xarici asılılığın azaldılmasını və milli proqram həllərinin inkişafını prioritet hədəf kimi müəyyən etmişdir. XXI əsrin texnoloji reallıqları fonunda proqram mühəndisliyinə strateji sahə kimi yanaşmayan ölkələr, qlobal rəqabətdə geri qalmaqla yanaşı, öz rəqəmsal gələcəklərini xarici korporasiyaların və dövlətlərin ixtiyarına vermək riski ilə üzləşirlər.

Bu tədqiqatın məqsədi müasir akademik nəşrlər əsasında milli proqram mühəndisliyinin inkişafı ilə dövlətin kibertəhlükəsizlik səviyyəsi arasındakı qarşılıqlı əlaqənin sistematik təhlilidir. Tədqiqat aşağıdakı suallara cavab verməyə çalışır: Kibertəhlükəsizliyin proqram mühəndisliyindən asılılığının əsas mexanizmləri hansılardır və kritik proqram sistemlərinin hazırlanmasında milli kadrların olmaması hansı riskləri yaradır?

## II. MİLLİ PROQRAM MÜHƏNDİSLİYİ VƏ KİBERSUVERENLİK

Müasir dövrdə dövlət institutlarının və kritik informasiya infrastrukturunun (Kİİ) sürətli rəqəmsal transformasiyası proqram təminatından yüksək və sistemli asılılıq formalaşdırmışdır. Milli proqram platformalarının yetərincə inkişaf etməməsi Kİİ-nin dayanıqlılığına və milli təhlükəsizliyin təmin olunmasına ciddi təhdidlər yaradır.

Xarici proqram təminatından asılılıq milli təhlükəsizlik üçün çoxşaxəli risklər formalaşdırır. İdxal olunan proqram sistemləri gizli funksional imkanlara malik ola bilər ki, bu da onların casusluq və ya diversiya məqsədləri üçün istifadəsi ehtimalını artırır və nəticə etibarilə kritik informasiya infrastrukturunun etibarlı fəaliyyətini təhlükə altına alır. Bununla yanaşı, xarici proqram təminatından istifadə rəqəmsal aktivlərin idarə olunması üzərində institusional nəzarətin məhdudlaşmasına səbəb olur və dövlətin öz informasiya resurslarını müstəqil şəkildə idarə etmə qabiliyyətini zəiflədir. Bu kontekstdə "rəqəmsal kolonializm" (Digital Colonialism) fenomeni xüsusi aktuallıq kəsb edir və xarici texnoloji ekosistemlərdən, standartlardan və platformalardan asılılığın strateji risklərini ön plana çıxarır. Qeyd olunan çağırışların aradan qaldırılması üçün milli əməliyyat sistemlərinin,

DOI: 10.25045/cyber.gov.2026.23

verilənlər bazası idarəetmə sistemlərinin və kibertəhlükəsizlik alətlərinin işlənməsi və tətbiqi texnoloji suverenliyin təmin olunmasının əsas şərtlərindən biri kimi çıxış edir.

Kiberhücumların intensivləşməsi və rəqəmsal üstünlük uğrunda qlobal rəqabətin kəskinləşməsi fonunda yerli texnologiyaların inkişafına yönəldilən investisiyalar dövlətin uzunmüddətli təhlükəsizliyinin, texnoloji müstəqilliyinin və strateji sabitliyinin təmin edilməsində həlledici əhəmiyyət kəsb edir.

Weir və həmmüəllifləri tərəfindən proqram təminatı, kibertəhlükəsizlik və kritik infrastruktur sahəsində 22 ekspertin iştirakı ilə Delphi metodu ilə aparılan tədqiqata görə, 2040-cı ilə qədər olan dövrdə KMİ üçün ən əhəmiyyətli təhlükə proqram təminatı qəzalarından və kiberhücumlardan sonra bərpa ilə bağlı insan yönümlü problemlərdir [1]. Yadav Avropa milli kiber-müdafiə təşkilatı haqqında tədqiqatında qeyd edir ki, "bulud texnologiya həllərinin sərhəd xarakteri və suveren olmayan vendorlardan asılılıq kiber-müdafiə təşkilatlarını rəqəmsal məkanda nəzarəti bərpa etmək və saxlamaq üçün sürətli rəqəmsallaşmaya sövq etmişdir" [2]. Bu asılılıq həm sülh, həm də müharibə dövründə istifadə edilə biləcək strateji zəifliklər yaradır.

Katsikas kibersuverenliyi "bir millətin və ya millətlər qrupunun rəqəmsal dünyada müstəqil fəaliyyət göstərmək qabiliyyəti" kimi təyin edir və bu anlayışın həm müdafiə mexanizmlərini, həm də rəqəmsal innovasiyaları stimullaşdıran hücum alətlərini əhatə etdiyini vurğulayır [3]. Bu perspektiv rəqəmsal suverenlik ilə kibertəhlükəsizlik arasındakı daxili əlaqəni vurğulayır. Rəqəmsal suverenlik passiv qorunma vəziyyəti deyil, dövlətin milli maraqlarına uyğun olaraq kritik rəqəmsal texnologiyalara nəzarət etmək, işləyib hazırlamaq və dəyişdirmək üçün aktiv qabiliyyətidir.

Kibertəhlükəsizlik strategiyaları, bir qayda olaraq, mövcud proqram təminatına tətbiq edilən periferik müdafiə mexanizmləri (müdaxilənin aşkarlanması sistemləri (IDS), antivirus proqramları və s.) ilə məhdudlaşırdı. Lakin müasir kiber-təhdid mənzərəsinin təhlili göstərir ki, ən effektiv müdafiə strategiyasının işlənməsi üçün proqram təminatının həyat dövrünün bütün mərhələlərində təhlükəsizlik prinsiplərinin sistemli inteqrasiyası zəruridir. Klare və həmmüəllifləri vurğulayırlar ki, "proqram təminatının həyat dövrü modelləri rəqəmsal suverenliyi nəzərə alaraq PT-nin işlənməsində nəzərə alınmalıdır" [4].

Bu, təhlükəsizliyin reaktiv modelindən (təhlükələrin aşkarlanması və onlara reaksiya) proaktiv modelə (təhlükəsizliyin ilkin mərhələlərdən başlayaraq layihələndirilməsi) keçid deməkdir. Bu baxımdan, proqram təminatının həyat dövrünün ilk mərhələlərindən etibarən təhlükəsizlik prinsiplərinin milli maraqlar və müstəqillik çərçivəsində layihələndirilməsi, xarici müdaxilələrə qarşı davamlılığı təmin edir. Yalnız xarici məhsullara əsaslanan reaktiv tədbirlərlə rəqəmsal suverenliyi qorumaq mümkün deyil; bunun üçün milli səviyyədə dərin texniki səriştəyə malik, təhlükəsiz məhsullarının işlənməsi üçün ekosistem yaratmaq zəruridir. Proaktiv təhlükəsizlik modelinə keçid, yalnız yeni alətlərin tətbiqi deyil, həm də insan kapitalının keyfiyyətcə dəyişməsini tələb edir. Bu yeni yanaşma, proqram mühəndislərindən, sistem analitiklərindən və layihə menecerlərindən təhlükəsiz proqram təminatı hazırlanması sahəsində dərin bilik və təcrübələrə malik olmağı zəruri edir.

Proqram mühəndisliyi kontekstində kibersuverenlik dövlətin kritik infrastrukturun fəaliyyətini təmin edən proqram təminatının yerli imkanlar hesabına layihələndirilməsi, monitorinqi və uzunmüddətli dəstəklənməsi bacarığıdır. Bu, təkcə texniki imkanları deyil, həm də ixtisaslı mütəxəssislərin, təhsil proqramlarının, tədqiqat mərkəzlərinin və rəqabətqabiliyyətli proqram məhsullarının hazırlanması üçün sənaye bazasının olmasını əhatə edir.

Milli Kiber-Müdafiə Konsepsiyasının mərkəzi sütununu hərbi sənayedə xarici asılılığın azaldılması və yerli proqram mühəndisliyi məhsullarının tətbiqi təşkil etməlidir. Xüsusilə komanda-idarəetmə sistemləri, Pilotsuz Uçuş Aparatlarının (PUA) alqoritmləri və qapalı rabitə şəbəkələri üçün milli mənbə koduna malik proqram platformalarının hazırlanması, hərbi texnikanın "gizli girişlər" (backdoor) və ya kənar müdaxilələr vasitəsilə iflic edilməsi riskini sıfıra endirir. Beləliklə, milli proqram təminatı sənayesinin inkişafı yalnız iqtisadi dividend deyil, həm də dövlətin müdafiə qabiliyyətinin rəqəmsal toxunulmazlığını təmin edən hərbi-strateji sığorta mexanizmidir. Hərbi doktrinalarda "Pre-positioning" (əvvəlcədən yerləşdirmə) anlayışı mövcuddur. Sülh dövründə xarici tədarükçülərdən alınan proqram təminatının və ya qurğuların (məsələn, marşrutlayıcılar) içərisinə gizli girişlər yerləşdirilir. Aktiv müharibə başladığı anda bu "yatmış" kodlar aktivləşdirilərək düşmən ölkənin elektrik şəbəkəsini, hava hücumundan müdafiə sistemlərini və rabitəsini bir anda söndürmək üçün istifadə edilir. Bu nümunələr sübut edir ki, hərbi suverenlik artıq yalnız sərhədlərin qorunması ilə deyil, həm də "kod suverenliyi" ilə ölçülür. Dövlətin hərbi infrastrukturunun xarici proqram təminatı üzərində qurulması, əslində düşmənə "qapının açarını" sülh dövründə vermək deməkdir.

## III. XARİCİ PROQRAM MƏHSULLARININ YARATDIĞI RİSKLƏR

Milli kibermüdafiə sistemlərinin qurulmasında rast gəlinən xarici təchizatçıdan asılılıq ("vendor lock-in") probleminin dövlətin rəqəmsal ekosistemi üçün yaratdığı fundamental təhdidlər m[vcuddur. Dövlətin kritik infrastrukturunun xarici mənşəli proqram sistemləri (PS) üzərində cəmlənməsi, milli təhlükəsizlik müstəvisində aşağıdakı dörd kateqoriya üzrə sistemli risklər yaradır:

*1) Texnoloji:* Xarici təchizatçıdan asılılıq dövlətin öz spesifik milli ehtiyaclarına uyğun texnoloji dəyişikliklər etmək imkanını məhdudlaşdırır. Dinamik kiber-təhdid mənzərəsində təhlükəsizlik sistemlərinin operativ qaydada adaptasiyası zəruridir. Mənbə koduna və daxili arxitekturaya birbaşa müdaxilə imkanının olmaması, dövləti təchizatçının yeniləmə qrafikindən və texniki razılığından asılı vəziyyətə salır [5].

*2) İqtisadi:* Lisenziyalaşdırma, texniki dəstək və zəruri yeniləmələr üzrə xərclərin təchizatçı tərəfindən birtərəfli qaydada dəyişdirilməsi, dövlət büdcəsinin planlaşdırılmasında qeyri-sabitlik yaradır və uzunmüddətli perspektivdə əhəmiyyətli maliyyə itkilərinə səbəb olur [6].

*3) Geosiyasi:* Xarici təchizatçılar mənsub olduqları ölkələrin dövlət maraqlarının və sanksiya siyasətlərinin təsir dairəsindədir. Geosiyasi gərginliklər zamanı təchizatçının xidməti dayandırması və ya yeniləmələri bloklaması kritik dövlət infrastrukturunu iflic edə bilər ki, bu da milli suverenlik üçün birbaşa təhdiddir [7].

*4) Gizli təhdidlər:* Mənbə koduna giriş olmadan dövlət casusluq və ya sabotaj üçün istifadə edilə biləcək qəsdən yaradılmış boşluqların və ya "əlavələrin" olmamasına zəmanət verə bilməz. Mənbə koduna girişin və audit imkanının olmaması, sistemin daxili təhlükəsizliyini "qara qutu" prinsipi ilə idarə etmək məcburiyyəti yaradır [8].

## IV. MİLLİ PROQRAM MÜHƏNDİSLİYİ SAHƏSİNDƏ PROBLEMLƏR

Aparılan sistemli təhlil göstərir ki, milli proqram mühəndisliyi sahəsində aşağıda göstərilən problemlər mövcuddur:

- Kadr çatışmazlığı. Yüksək ixtisaslı, beynəlxalq səviyyədə rəqabətədavamlı proqram məhsulları yarada bilən mütəxəssislərin məhdudluğu, eləcə də "beyin axını" fenomeni insan kapitalının davamlı inkişafına ciddi maneə yaradır. Bu amil innovasiya potensialının zəifləməsinə və yerli texnoloji təşəbbüslərin miqyaslanmasının çətinləşməsinə səbəb olur.
- Texnoloji gerilik. Fundamental və tətbiqi tədqiqatların yetərincə inkişaf etməməsi, xüsusilə süni intellekt, kvant hesablamaları və digər qabaqcıl texnologiyalar sahəsində mövcud boşluqlar milli texnoloji müstəqilliyin formalaşmasını ləngidir.
- Ekosistemin fraqmentasiyası. Vahid standartların, qarşılıqlı uyğunluq prinsiplərinin və inteqrasiya olunmuş platformaların çatışmazlığı nəticəsində bir-birindən təcrid olunmuş proqram həlləri formalaşır. Bu isə resursların səmərəsiz istifadəsinə və sistemlərin kompleks şəkildə inkişafının qarşısının alınmasına gətirib çıxarır.
- İqtisadi amillər. Qlobal texnoloji korporasiyalarla rəqabətin yüksək olması, vençur kapitalının məhdudluğu və yerli proqram məhsullarının kommersiyalaşdırılması prosesində mövcud institusional və bazar maneələri yerli proqram məhsulların bazara çıxışını çətinləşdirir.

Milli proqram mühəndisliyinin inkişafı və təhlükəsiz proqram təminatının yaradılması çoxsəviyyəli yanaşma tələb edir. Bu kontekstdə proqram mühəndisliyi üzrə bilik və bacarıqların formalaşdırılması aşağıdakı əsas səviyyələri əhatə edir [9]:

Təhsil səviyyəsi. Universitetlər və texniki təhsil müəssisələri proqram mühəndisliyinin tədrisinə kibertəhlükəsizlik prinsiplərini sistemli şəkildə inteqrasiya etməlidirlər. Bu yanaşma kibertəhlükəsizliyin ayrıca fənn kimi deyil, proqram təminatının hazırlanmasının bütün mərhələlərini əhatə edən komponent kimi tədrisini nəzərdə tutur.

Peşəkar səviyyə. Təcrübəli proqram mühəndisləri üçün müasir kiber təhdidlər, boşluqların idarə olunması və qabaqlayıcı müdafiə mexanizmləri üzrə davamlı peşəkar inkişaf proqramlarının təşkili zəruridir. Xüsusilə kritik informasiya infrastrukturu ilə əlaqəli sistemlər üzərində çalışan mütəxəssislər üçün təhlükəsiz proqramlaşdırma üzrə sertifikatlaşdırma mexanizmlərinin tətbiqi standartlaşdırılmış tələblərdən biri kimi çıxış etməlidir.

Tədqiqat səviyyəsi. Milli tədqiqat institutları və laboratoriyalar proqram təminatının təhlükəsizliyi sahəsində həm fundamental, həm də tətbiqi tədqiqatları genişləndirməlidirlər. Bu istiqamətdə əsas prioritetlərə proqram təminatının verifikasiyası və validasiyası, boşluqların avtomatlaşdırılmış aşkarlanması, dinamik və statik analiz metodlarının inkişafı, eləcə də yeni nəsil müdafiə mexanizmlərinin işlənməsi daxildir.

## V. MİLLİ PROQRAM MÜHƏNDİSLİYİNİN İNKİŞAFI ÜZRƏ TÖVSİYYƏLƏR

Tədqiqatların təhlilinə əsasən, milli proqram mühəndisliyinin inkişafı vasitəsilə rəqəmsal suverenliyə nail olmaq üçün Cədvəl 1-də göstərilən şoxsəviyyəli inkişaf strategiyası təklif edilmişdir.

CƏDVƏL 1. MİLLİ PROQRAM MÜHƏNDİSLİYİNİN İNKİŞAF STRATEGİYASI

| **Səviyyə** | **Komponent** | **Konkret Tədbirlər** |
|---|---|---|
| Təhsil | Kadr hazırlığı | Kibertəhlükəsizliyin informatika və PM proqramlarına inteqrasiyası; təhlükəsiz PT hazırlanması üzrə ixtisaslaşdırılmış proqramların yaradılması; təcrübəli mütəxəssislər üçün davamlı tədris proqramları [10] |
| Sənaye | İstehsal gücləri | Kritik infrastruktur üçün yerli proqram məhsulları hazırlayan şirkətlərə dəstək; dövlət satınalmalarında yerli PT istifadəsi tələbləri; texnopark və inkubatorların yaradılması |
| Tənzim-ləyici | Qanunvericilik və standartlar | Təhlükəsiz PT hazırlanması üzrə milli standartların işlənib hazırlanması, Kİİ-də xarici proqram məhsulları istifadəsinin tənzimlənməsi [11] |
| Təşkilati | İdarəetmə və koordinasiya | PM-in inkişafının koordinasiyası üzrə milli orqanın yaradılması; dövlət qurumları arası əməkdaşlıq; dövlət-özəl sektor tərəfdaşlığı |

Bununla yanaşı, milli proqram mühəndisliyinin inkişafı üzrə strategiyanın effektiv reallaşdırılması üçün dövlət dəstəyi həlledici rol oynayır. Bu istiqamətdə aşağıdakı maliyyə və institusional tədbirlərin həyata keçirilməsi zəruridir:

- Qrant və subsidiyalar. Bu maliyyə alətləri innovativ fəaliyyətin stimullaşdırılmasına, elmi-tədqiqat və təcrübi-konstruktor işlərinin genişləndirilməsinə, eləcə də yeni proqram məhsullarının işlənilməsi ilə bağlı risklərin azaldılmasına xidmət edir.

- Tənzimləyici güzəştlər. Dövlət sektorunda və strateji əhəmiyyətli sahələrdə yerli proqram təminatına üstünlük verilməsini təşviq edən normativ-hüquqi mexanizmlərin tətbiqi daxili bazarın formalaşmasına və milli məhsulların yayılmasına şərait yaradır.
- Kiçik və orta sahibkarlığın dəstəklənməsi. İnnovasiyanın əsas mənbələrindən biri olan kiçik və orta proqram təminatı istehsalçıları üçün vergi güzəştləri, inkubasiya proqramları və texnoloji parkların yaradılması onların inkişafını sürətləndirir və bazara çıxış imkanlarını genişləndirir.

Maliyyə və tənzimləyici tədbirlərin kompleks şəkildə tətbiqi yerli proqram sənayesinin inkişafı üçün dayanıqlı iqtisadi və institusional mühit formalaşdırır, onun beynəlxalq rəqabət qabiliyyətini artırır və texnoloji suverenliyin təmin olunmasına xidmət edir [12].

## NƏTİCƏ

Aparılan təhlil göstərir ki, dövlətin kibertəhlükəsizliyi birbaşa olaraq milli proqram mühəndisliyinin inkişaf səviyyəsindən asılıdır. Bu asılılıq texnoloji, təşkilati və strateji səviyyələrdə özünü göstərir və təhlükəsiz, dayanıqlı rəqəmsal mühitin formalaşdırılmasını şərtləndirir.

Gələcək tədqiqatlar rəqəmsal suverenliyin ölçülməsi üçün metrikaların işlənməsinə, milli strategiyaların effektivliyinin qiymətləndirilməsinə və təhlükəsiz proqram məhsullarının işlənməsində intellektual texnologiyaların tətbiqinə yönəldilməlidir.

## ƏDƏBİYYAT


[1] C. Weir, C. Loureiro-Koechlin, L. Hunt, and L. Dennis, "The human factor: Addressing computing risks for critical national infrastructure towards 2040," *Computers & Security*, vol. 157, p. 104524, 2025, doi: 10.1016/j.cose.2025.104524.

[2] Y. S. Yadav, "Agile organizing of national cyber defence capabilities: Decoupling external dependencies and catalysing digital sovereignty," *Procedia Computer Science*, vol. 254, pp. 260–268, 2025, doi: 10.1016/j.procs.2025.02.085.

[3] S. K. Katsikas, "Towards a cybersecurity-oriented research agenda for digital sovereignty," *Procedia Computer Science*, vol. 254, pp. 279–288, 2025, doi: 10.1016/j.procs.2025.02.087.

[4] M. Klare, R. Hrestic, A. Stelter, and U. Lechner, "Digital sovereignty and digital transformation: Practice recommendation for the software life cycle process," *Procedia Computer Science*, vol. 254, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/-pii/S1877050925004314

[5] A. Andreoli *et al*., "On the prevalence of software supply chain attacks: Empirical study and investigative framework," *Forensic Science International: Digital Investigation*, vol. 44, p. 301508, 2023.

[6] G. Robles *et al*., "A comparative analysis of industrial involvement and licensing in the open source software ecosystems of four IoT standards," *Journal of Systems and Software*, p. 112708, 2025.

[7] S. Kergroach and M. M. Bianchini, *The Digital Transformation of SMEs*. Paris, France: Organisation for Economic Co-operation and Development, 2021. [Online]. Available: http://www.sela.org/media/3222564/the-digital-transformation-of-smes.pdf

[8] E. Balsa, H. Nissenbaum, and S. Park, "Cryptography, trust and privacy: It's complicated," in *Proc. Symp. Computer Science and Law*, 2022, pp. 167–179.

[9] C. Topping, A. Dwyer, O. Michalec, B. Craggs, and A. Rashid, "Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks," *Computers & Security*, vol. 108, p. 102324, 2021, doi: 10.1016/j.cose.2021.102324.

[10] T. Kazimov and T. Bayramova, "Problems of teaching software engineering in Azerbaijan," *Problems of Information Society*, vol. 8, no. 1, pp. 92–96, 2017.

[11] T. A. Bayramova, "Analysis of software engineering standards," *Problems of Information Society*, vol. 11, no. 1, pp. 83–95, 2020.

[12] M. Dawson, P. Taveras, and D. Taylor, "Applying software assurance and cybersecurity NICE job tasks through secure software engineering labs," *Procedia Computer Science*, vol. 153, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S187705091932226


## Problems of Formation of National Software Engineering to Ensure Cyber Sovereignty of the State


**Tamilla Bayramova**

Institute of Information Technology, Baku, Azerbaijan



**Abstract**— The research work is devoted to the analysis of the role of national software engineering in ensuring cyber sovereignty and digital independence of the state against the background of modern geopolitical challenges. The paper examines the risks posed by dependence on foreign software systems for national security, including the vulnerability of critical infrastructure and loss of control over digital assets. The formation of national technological platforms, a national digital ecosystem and highly qualified personnel potential is justified as one of the fundamental conditions for cyber sovereignty. The paper puts forward recommendations on state support mechanisms that stimulate the development of national software engineering, modernization of the educational base and integration of cybersecurity principles in the software lifecycle.



**Keywords**— cybersecurity; software engineering; digital sovereignty; critical infrastructure; supply chain security; dependency management.