“DÖVLƏTİN KİBERSUVERENLİYİNİN TƏMİN OLUNMASININ ELMİ-PRAKTİKİ PROBLEMLƏRİ” RESPUBLİKA KONFRANSI

P R O Q R A M

KONFRANSIN AÇILIŞ MƏRASİMİ

Böyük konfrans zalı, 11:00 – 12:30

- AMEA-nın vitse-prezidenti, ETN İnformasiya Texnologiyaları İnstitutunun baş direktoru, **akademik Rasim Əliquliyev**
- Azərbaycan Respublikası Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyasının rəisi, **general-mayor Elşad Nəsirov**
- Azərbaycan Respublikası Dövlət Təhlükəsizliyi Xidmətinin Milli Kibertəhlükəsizlik Mərkəzinin rəisi, **general-mayor Davud Rüstəmov**
- Azərbaycan Texniki Universitetinin rektoru, **professor Vilayət Vəliyev**
- Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin Baş idarə rəisinin müavini, **polkovnik-leytenant Tural Məmmədov**
- Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyasının İdarə Heyətinin sədri **Pənah Musayev**
- Azərbaycanda İnternetin İnkişafı Forumunun prezidenti, Multimedia Mərkəzinin direktoru **Osman Gündüz**

I SEKSİYA

DÖVLƏTİN KİBERSUVERENLİYİNİN

TƏMİN OLUNMASININ ELMİ-TEXNOLOJİ ASPEKTLƏRİ

Böyük konfrans zalı, saat 14:00–17:30

Həmsədrlər: AMEA-nın müxbir üzvü Ramiz Alıquliyev,
texnika elmləri doktoru Yadigar İmamverdiyev

Elmi katib: texnika elmləri üzrə fəlsəfə doktoru Fərqanə Abdullayeva

1. Rasim Əliquliyev, Ramiz Alıquliyev, Fərhad Yusifov

Dayanıqlı və təhlükəsiz rəqəmsal arxitektura dövlətin kibersuverenliyinin qarantıdır

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat işi Azərbaycanda yeni rəqəmsal arxitekturanın formalaşdırılmasının zəruriyyəti və qlobal texnoloji çağırışlar kontekstində onun elmi-texnoloji əsaslarının işlənməsi məsələsinə həsr olunmuşdur. Bu məqsədlə yeni reallıqlar şəraitində rəqəmsal dövlətin formalaşdırılmasına yürüdülən və mühüm əhəmiyyət kəsb edən bir sıra arxitektur tələblər irəli sürülmüşdür. Göstərilmişdir ki, rəqəmsal dövlətin formalaşdırılması və inkişafı həmin arxitektur tələblər əsasında həyata keçirilərsə, bu virtual məkanda dövlətin kibersuverenliyi üçün ciddi güvənlik yaranar.

2. Lalə Kərimova

Azərbaycanın rəqəmsal suverenlik indeksi: analitik və metodoloji yanaşma

Azərbaycan Respublikası Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi

Tədqiqat işində rəqəmsal suverenlik anlayışının ölçüləbilən və idarəolunan alətə çevrilməsinə dair yanaşma təhlil edilir. Araşdırmada beynəlxalq təcrübədə mövcud olan konseptual və indikator-əsaslı modellər müqayisə olunur, onların üstün və məhdud cəhətləri müəyyənləşdirilir. İşdə Azərbaycanın Rəqəmsal

Suverenlik İndeksinin metodologiyası təqdim olunur. Təklif olunan model rəqəmsal infrastruktur, məlumat, texnologiya, tənzimləmə, insan kapitalı və kiberdayanıqlılıq aspektlərini inteqrə olunmuş şəkildə qiymətləndirməyə imkan yaradır.

3. **Ramiz Alıquliyev**

Dövlətin data suverenliyi: problemlər, konseptual yanaşmalar və perspektivlər

ETN İnformasiya Texnologiyaları İnstitutu

Rəqəmsal erada datanın strateji resurs statusu qazanması dövlətin milli təhlükəsizliyi, iqtisadi müstəqilliyi, kibersuverenliyi və s. kontekstdə "data suverenliyi" anlayışını ön plana çıxarmışdır. Tədqiqat işində əvvəlcə "data müstəmləkəçiliyi" anlayışının mahiyyəti, məqsədi və dünyanın nəhəng data imperiyaları haqqında məlumat verilmiş, sonra dövlətin data suverenliyinin formalaşması prosesi, bu sahədə qarşıya çıxan əsas hüquqi, texnoloji və siyasi problemlər təhlil edilmişdir. Tədqiqat çərçivəsində transsərhəd data axınlarının tənzimlənməsi, xarici platformalardan asılılıq və s. kimi məsələlərə konseptual yanaşmalar nəzərdən keçirilmişdir. Data suverenliyi sahəsində beynəlxalq təcrübə araşdırılmış, milli data ekosisteminin formalaşması üçün konseptual yanaşma təklif olunmuşdur.

4. **Sərxan Mirili**

Dövlətin data və bulud suverenliyinin təmin olunmasında kibertəhlükəsizlik risklərinin analizi və praktik yanaşmalar

DTX-nin Heydər Əliyev adına Akademiyası

Rəqəmsal transformasiya prosesləri dövlət idarəçiliyində bulud texnologiyalarının geniş tətbiqini şərtləndirmişdir. Bu proses dövlət xidmətlərinin səmərəliliyini artırmaqla yanaşı, data və bulud suverenliyinin təmin olunması baxımından yeni kibertəhlükəsizlik riskləri formalaşdırır. Tədqiqat işində dövlət sektorunda istifadə olunan bulud əsaslı informasiya sistemlərində mövcud olan kibertəhlükəsizlik riskləri təhlil edilir və bu risklərin data suverenliyinə təsiri qiymətləndirilir. Eyni zamanda, dövlətin data və bulud suverenliyinin təmin olunması məqsədilə konseptual və

praktik kibertəhlükəsizlik yanaşmaları təklif olunur. Tədqiqatın nəticələri etibarlı və dayanıqlı rəqəmsal dövlət sistemlərinin formalaşdırılması baxımından elmi-praktiki əhəmiyyət daşıyır.

5. **Rəşid Ələkbərov**

Şəbəkə-kommunikasiya infrastrukturunun suverenliyi: problemlər, təhlükəsizlik məsələləri, risklər və həlli yolları

ETN İnformasiya Texnologiyaları İnstitutu

Müasir dövrdə şəbəkə-kommunikasiya suverenliyi dövlətlərin milli təhlükəsizliyi və rəqəmsal inkişafı üçün strateji əhəmiyyət daşıyır. Tədqiqat işində şəbəkə-kommunikasiya suverenliyinin mövcud vəziyyəti, aktual problemləri, təhdidlər, risklər və əsas komponentləri təhlil edilir. Həmçinin, milli rəqəmsal müstəqilliyin təmin olunması üçün tövsiyə olunan həll yolları təqdim olunur. Araşdırma göstərir ki, hüquqi baza, texnoloji infrastruktur, məlumat təhlükəsizliyi, kadr potensialı, iqtisadi resurslar və ictimai maarifləndirmə sahələrinin gücləndirilməsi şəbəkə-kommunikasiya suverenliyinin effektiv qorunmasını təmin edir.

6. **Rəşad Nuriyev**

Rəqəmsal məhkəmə ekspertizasının kibersuverenliyin təmin olunmasında yeri və rolu

Azərbaycan Respublikası Ədliyyə Nazirliyinin Məhkəmə Ekspertizası Mərkəzi

Tədqiqat işində rəqəmsal məhkəmə ekspertizasının hüquqi mahiyyəti, onun vasitəsilə həll olunan əsas məsələlər, habelə rəqəmsal sübutların istintaq və ədalət mühakiməsində tətbiqi məsələləri araşdırılır. Azərbaycan Respublikasının mövcud qanunvericiliyi kontekstində rəqəmsal ekspertizanın kibersuverenliyin təmin olunmasında, informasiya təhlükəsizliyinə yönəlmiş təhdidlərin müəyyənləşdirilməsində və cinayət işləri üzrə sübutetmə prosesinə töhfəsi təhlil olunur. Rəqəmsal ekspertizanın digər elmi və texniki sahələrlə qarşılıqlı əlaqəsi, habelə bu sahənin müasir inkişaf tendensiyaları və perspektivləri ümumiləşdirilmiş şəkildə araşdırılır.

7. **Рамиз Алыгулиев, Людмила Сухостат**

Киберсуверенитет государства и критические инфраструктуры: проблемы и пути их решения

Институт Информационных Технологий МНО

В данном исследовании анализируются текущие проблемы безопасности критических инфраструктур с целью обеспечения киберсуверенитета, включая различные уязвимости и угрозы. Исследуются международный опыт и стандарты обеспечения кибербезопасности и киберустойчивости критических инфраструктур. Данное исследование может помочь в обеспечении кибербезопасности и киберустойчивости критических инфраструктур, обеспечивая конфиденциальность, автономию и доверие, которые необходимы для поддержания цифрового суверенитета. Данная работа предоставляет ценные сведения для будущих исследований по разработке адаптивных и надежных решений, обеспечивающих безопасность децентрализованных систем и укрепляющих принципы цифрового суверенитета государств.

8. **Yadigar İmamverdiyev, Ağa Ağayev**

Milli kibersuverenlik üçün kriptoqrafiya yol xəritəsi

Azərbaycan Texniki Universiteti

Tədqiqat işində milli kibersuverenliyin təmin olunmasında kriptoqrafiyanın strateji rolu əsaslandırılır və dövlət səviyyəsində kriptoqrafik imkanların sistemli inkişafı üçün "Milli kriptoqrafiya yol xəritəsi" konseptual modeli təklif olunur. Yol xəritəsi modeli kriptoqrafiyanı yalnız texniki alət kimi deyil, hüquqi-normativ baza, institusional idarəetmə, standartlaşdırma, texnoloji infrastruktur (açar idarəetməsi), elmi-tədqiqat və kriptoanaliz, insan kapitalı, eləcə də sənaye və yerli məhsul ekosistemi ilə birlikdə milli səviyyədə idarə olunan kompleks sistem kimi təqdim edir. Tədqiqat işində simmetrik kriptoqrafiyanın yol xəritəsində xüsusi yer tutduğu qeyd olunur və bu sahədə perspektiv inkişaf mərhələləri göstərilir.

9. **Ramiz Şıxəliyev**

Dövlətin kiberimmunitetinin analizi və yüksəldilməsi yolları

ETN İnformasiya Texnologiyaları İnstitutu

İnformasiya-kommunikasiya texnologiyalarının sürətli inkişafı yeni mürəkkəb, çoxvektorlu və süni intellekt əsaslı kiberhücumların yaranmasına gətirib çıxarmışdır. Ənənəvi reaktiv müdafiə modelləri bu kiberhücumlara qarşı o qədər də effektiv deyil. Buna görə, kiberimmunitet dövlət informasiya sistemlərinin adaptiv, proaktiv və özü öyrənən mexanizmlərlə kibertəhlükəsizliyini təmin edən strateji yanaşma kimi aktuallaşır. Bioloji immun sistemin prinsiplərinə əsaslanaraq, kiberimmunitet erkən aşkarlama, adaptiv reaksiya, immun yaddaş və öz-özünü bərpa imkanlarını birləşdirərək milli kibersuverenliyin təmin edilməsinə imkan verər. Tədqiqat işində mövcud kibertəhdidlərin xüsusiyyətləri və ənənəvi reaktiv kibertəhlükəsizlik yanaşmalarının məhdudiyyətləri analiz edilir və dövlətin kiberimmunitetnin yüksəldilməsi yolları araşdırılır.

10. **Şakir Mehdiyev, Lalə Mehdiyeva**

Texnoloji Suverenlik: qlobal çağırışlar, təhlükələr və risklər

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat işində texnoloji suverenlik anlayışının müasir qlobal sistemdə formalaşması və transformasiyası təhlil edilir. Geosiyasi qeyri-müəyyənlik, texnoloji zəncirlərin fraqmentasiyası və rəqəmsal transformasiyanın sürətlənməsi fonunda texnoloji suverenliyin dövlətlərin milli təhlükəsizliyi və dayanıqlı inkişaf strategiyalarındakı rolu araşdırılır. Texnoloji suverenliyin konseptual məzmunu, dövlət suverenliyi strukturundakı yeri və əsas yanaşmaları sistemləşdirilir. Müxtəlif ölkələrin təcrübəsi əsasında texnoloji suverenliyin reallaşdırılma modelləri, habelə bu proseslə bağlı risklər və məhdudiyyətlər qiymətləndirilir. Texnoloji suverenliyin yalnız texnologiyaların lokallaşdırılması ilə deyil, elmi-tədqiqat potensialı, insan kapitalı, innovasiya ekosistemi və kiberdayanıqlılığın inteqrasiyası əsasında formalaşan çoxölçülü strateji anlayış olduğu əsaslandırılır.

11. Araz Mustafa

Sosial təyinatlı kiberfiziki sistemlərdə fərdi məlumatların transsərhəd ötürülməsi risklərinin çoxmeyarlı qiymətləndirilməsi

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat işində sosial təyinatlı kiberfiziki sistemlərdə toplanan fərdi məlumatların ötürülməsi zamanı yaranan risklərin qiymətləndirilməsi üçün çoxmeyarlı yanaşma təklif edilir. Baxılan yanaşmada texnoloji boşluqlarla yanaşı, sosial mühit, insan amili, hüquqi tənzimləmə səviyyəsi və milli rəqəmsal infrastrukturun dayanıqlılığı kimi faktorlar da nəzərə alınır. Risklərin prioritetləşdirilməsi məqsədilə müasir qərarqəbuletmə metodlarından istifadə edilərək zəifliklərin müəyyənləşdirilməsi və onların kibersuverenliyə potensial təsirinin qiymətləndirilməsi üçün yanaşma təklif olunur. Əldə olunan nəticələr sosial təyinatlı kiberfiziki sistemlərdə fərdi məlumatların konfidensiallığının qorunması ilə yanaşı, milli rəqəmsal mühitdə idarəetmə və nəzarət mexanizmlərinin gücləndirilməsinə, eləcə də kibersuverenliyin təmin edilməsinə xidmət edir.

12. Bəhruz Əliyev

Dövlətin kibersuverenliyinə çoxaspektli yanaşma

Bakı Dövlət Universiteti, Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyası

Tədqiqat işində dövlətin kibersuverenliyinin təmin olunmasına çoxaspektli yanaşma irəli sürülür. Bu kontekstdə milli rəqəmsal müstəqillik, ağıllı şəhər infrastrukturları, yeni nəsil (post-quantum) kriptoqrafiya, süni intellekt əsaslı müdafiə mexanizmləri və insan faktorunun strateji rolu sistemli şəkildə təhlil edilir. Kadr çatışmazlığı, təşkilati mədəniyyət və maarifləndirmə səviyyəsi risklərin reallaşma ehtimalını müəyyən edən əsas amillər kimi qiymətləndirilir. Kibersuverenliyin gücləndirilməsi üçün milli rəqəmsal proqram və texnologiyalara, dayanıqlı kriptoqrafik transformasiyaya, təhlükəsiz infrastruktur dizaynına, süni intellekt

ilə gücləndirilmiş müdafiəyə və insan kapitalının inkişafına əsaslanan konseptual yanaşma təklif olunur.

13. **Rasim Mahmudov**

Kibersuverenlik modelləri və onların müqayisəli təhlili

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat işində böyük dövlətlərin kibersuverenliyinin təmin edilməsi ilə bağlı ideoloji, hüquqi, texnoloji və siyasi müstəvilərdə fəaliyyəti müqayisəli şəkildə araşdırılır. Klassik ərazi yurisdiksiyasından fərqli olaraq kibersuverenliyin informasiya axını, platforma davranışı və texnoloji infrastruktur üzərində normativ nəzarət kimi formalaşmasının xüsusiyyətləri şərh olunur. Çin, ABŞ, Avropa Birliyi, Rusiya və Hindistanın kibersuverenlik modelləri hüquqi baza, texnoloji strategiya və diplomatik təşəbbüslər baxımından sistemli şəkildə analiz olunur. Tədqiqatda qlobal kibermühitin tənzimlənməsi sahəsində normativ parçalanmanın qarşısını almaq üçün çoxtərəfli tənzimləmə imkanlarına diqqət yetirilir və bu sahədə gələcək araşdırmalar üçün konseptual çərçivə təklif edilir.

14. **Babək Nəbiyev, Könül Daşdəmirova**

Rəqəmsal dövlət mühitində kibersuverenliyin təmin edilməsi və milli kibertəhlükəsizliyin konseptual modelinin işlənməsi

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat işində elektron dövlət mühitində kibersuverenliyin təmin edilməsi və milli kibertəhlükəsizliyin konseptual modelinin işlənməsi məsələləri araşdırılır. Qloballaşma şəraitində rəqəmsal asılılıqların yaratdığı risklər təhlil olunur, kibertəhlükəsizliyin idarə edilməsində Whole-of-Government və Whole-of-Society yanaşmalarının rolu əsaslandırılır. Tədqiqat çərçivəsində Milli Kibertəhlükəsizlik Sisteminin (MKTS) formalaşdırılması üçün texnoloji dayanıqlılıq, Secure-by-Design prinsipləri və proaktiv təhlükəsizlik yanaşmaları tədqiq edilir. Eyni zamanda, MKTS-in ölçülə bilən qiymətləndirilməsi məqsədilə Milli Kibertəhlükəsizlik İndeksinin çoxqatlı arxitekturası və proses modeli təklif olunur.

15. **Nərmin Adıgözəlova**

Dövlətin kibersuverenliyi sahəsində elmi araşdırmaların vəziyyəti, multidissiplinar təhlil, trendlər və perspektivlər

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat işində Scopus və Web of Science elmi bazalarında "Cyber Sovereignty" istiqamətində aparılmış tədqiqatlar təhlil edilmiş və dərc olunan əsərlərin bibliometrik analizi aparılmışdır. Bibliometrik analiz bu sahədə çap olunan əsərlərin illər, dillər, elm sahələri və coğrafi paylanması kimi göstəricilərinə əsasən aparılmışdır. O cümlədən, kibersuverenlik sahəsində elmi əsərlərin istinad analizi əsasında ranqlaşdırılması məsələsinə baxılmış, 2015-2025-ci illər ərzində bu istiqamətdə aparılan tədqiqatların nəticələri analiz edilmiş və mövcud problemlər müəyyən edilmişdir.

16. **Fərhad Yusifov**

Dövlətin kibersuverenliyinin ümumarxitektur prinsipləri və funksional komponentləri: problemlər və konseptual yanaşmalar

ETN İnformasiya Texnologiyaları İnstitutu

Dövlət idarəçiliyində rəqəmsal transformasiyalar və süni intellekt texnologiyalarının tətbiqi dövlətin kibersuverenliyinin təmin edilməsi baxımından yeni çağırışlar, təhdidlər və risklər yaradır. Tədqiqat işində dövlətin kibersuverenliyinin arxitektur prinsipləri və təklif olunan modellər araşdırılır. Aparılan tədqiqatlarda dövlətin kibersuverenliyinin səviyyələr üzrə strukturlaşdırılmasına dair fərqli yanaşmalar mövcuddur. Bu yanaşmalar əsasən texnoloji, infrastruktur, məlumatların idarə olunması və geosiyasi təsirlərin nəzərə alınması kimi komponentləri əhatə edir. Tədqiqat işində dövlətin kibersuverenliyinin təmin edilməsi üçün konseptual model təklif edilmişdir. Təklif olunan yanaşma texnoloji, idarəetmə və sosial səviyyələrdən ibarətdir və bu səviyyələr birlikdə ölkənin kibersuverenlik ekosistemini formalaşdırır.

17. **İradə Ələkbərova**

Dövlətin kibersuverenliyinin təmini üçün informasiya qarşıdurması strategiyalarının işlənməsi

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat işində müasir hibrid müharibələrin tərkib hissəsi olan informasiya qarşıdurması fonunda rəqəmsal dövlətin kibersuverenliyinin təmini məsələləri tədqiq olunur. Beynəlxalq təcrübə nəzərə alınaraq, kritik infrastrukturun kiberdayanıqlılığı və informasiya hücumlarının zəncirvari təsir mexanizmləri analiz edilir. Tədqiqat işində infrastruktur, informasiya, idarəetmə və hüquqi müstəviləri əhatə edən dörd mərhələli strateji model işlənib hazırlanmışdır. Tədqiqatın nəticələri rəqəmsal dövlətin suverenliyini təkcə texniki müdafiə ilə deyil, həm də aktiv informasiya qarşıdurması strategiyaları və rəqəmsal etimadın qorunması ilə əlaqələndirir.

18. **Günay İsgəndərli**

Rəqəmsal dövlət platformasında sosial təhlükəsizliyin qiymətləndirilməsi mexanizmləri

ETN İnformasiya Texnologiyaları İnstitutu

Müasir dövrdə rəqəmsal dövlət idarəçiliyi dövlət–vətəndaş münasibətlərini əsaslı şəkildə dəyişmiş və sosial təhlükəsizlik anlayışına yeni yanaşmalar tələb etmişdir. Rəqəmsal platformalar idarəetmədə operativliyi, şəffaflığı və xidmətlərin əlçatanlığını artırsa da, məmnunluğun təmin olunmaması sosial risklərin və idarəetmədə narazılığın artmasına səbəb ola bilər. Bu işdə sosial təhlükəsizlik dövlət və vətəndaş arasında qarşılıqlı məmnunluq balansı prizmasından tədqiq olunur. Təklif olunan konseptual-analitik model rəqəmsal dövlət platformalarında sosial riskləri erkən mərhələdə müəyyən etməyə, təşkilati zəiflikləri aşkar etməyə və idarəetmə qərarlarını elmi əsaslarla formalaşdırmağa imkan verir.

19. **Məmməd Həşimov**

Kvant texnologiyalarının dövlətin kibersuverenliyinin təmin edilməsində rolu: mövcud vəziyyət, problemlər və perspektivlər

ETN İnformasiya Texnologiyaları İnstitutu

Kvant texnologiyaları müasir informasiya sistemlərinin inkişafında yeni mərhələ formalaşdıraraq hesablama imkanlarını genişləndirir. Bu texnologiyalar xüsusilə kriptoqrafiya və milli kibertəhlükəsizlik infrastrukturu baxımından strateji əhəmiyyət daşıyır. Tədqiqat işində kvant texnologiyalarının kibersuverenlik kontekstində mövcud vəziyyəti təhlil edilir, onların mövcud kriptoqrafik mexanizmlər üçün yaratdığı risklər və texnoloji asılılıq kimi problemlər müəyyənləşdirilir. Bununla yanaşı, kvant texnologiyalarının milli kibertəhlükəsizlik arxitekturasının formalaşmasına və strateji planlaşdırma yanaşmalarına təsiri qiymətləndirilir. Eyni zamanda post-kvant kriptoqrafiyaya keçid, milli kvant strategiyalarının formalaşdırılması və normativ-hüquqi bazanın təkmilləşdirilməsi kibersuverenliyin təmin edilməsi istiqamətində əsas həll mexanizmləri kimi əsaslandırılır.

20. **Anar Suvarov**

The dark web and cyber sovereignty: risks to states and defense mechanisms

Azerbaijan State Oil and Industry University

This research examines the role of the Dark Web in contemporary cyberthreats and its impact on cybersovereignty. It analyzes cybercrime markets, cybercrime as a service, and key risks to states, such as data breaches and ransomware. The study also discusses defense mechanisms, including threat intelligence and dark web monitoring. The findings emphasize the significance of proactive cybersecurity approaches to protect national security.

21. Rəşid Ələkbərov, Oqtay Ələkbərov

Rəqəmsal dövlətin bulud suverenliyi: mövcud vəziyyət, problemlər, risklər və həlli yolları

ETN İnformasiya Texnologiyaları İnstitutu

Rəqəmsallaşmanın sürətlənməsi dövlət idarəçiliyində bulud texnologiyalarının geniş tətbiqinə səbəb olmuşdur. Lakin məlumatların xarici provayderlərdə saxlanması milli təhlükəsizlik, hüquqi müstəqillik və kibertəhlükəsizlik baxımından ciddi risklər yaradır. Bu səbəbdən "bulud suverenliyi" anlayışı rəqəmsal dövlət konsepsiyasının əsas sütunlarından birinə çevrilmişdir. İşdə bulud suverenliyinin konseptual əsasları, komponentləri, mövcud problemlər, təhlükələr və risklər təhlil olunur, həmçinin effektiv həll yolları təqdim edilir.

22. Adilə Kərimova

Dövlətin kibersuverenliyinin təmin olunmasında kibertəhdid kəşfiyyatı və əks-kəşfiyyatı texnologiyaları: konseptual yanaşmalar, arxitektur həllər və perspektivlər

Azərbaycan Texniki Universiteti

Dövlət səviyyəsində kibertəhdid kəşfiyyatı texnologiyaları kibertəhdidlərin erkən aşkarlanması, analizi, risk idarəetməsi və proaktiv müdafiə mexanizmlərinin formalaşmasını təmin edir. Əks-kəşfiyyat texnologiyaları isə dövlətin kibertəhlükəsizliyini təmin etmək üçün dövlətin informasiya resurslarını hədəf almış gizli fəaliyyətləri aşkarlayır, təhdid aktorlarını izləyir və kəşfiyyat fəaliyyətlərinə qarşı mübarizə aparır. Tədqiqat işində təklif edilən konseptual yanaşmada kibertəhdid kəşfiyyatı sisteminin arxitekturası strateji, operativ və taktiki səviyyədə strukturlaşdırılır və inteqrasiya olunmuş həllər əsasında qurulması nəzərdə tutulur. Sistemin sintezi üçün süni intellekt metod və alqoritmlərinin işlənməsi dövlətin kibertəhlükəsizliyinin dayanıqlığının təmin olunmasına və kibersuverenliyin gücləndirilməsinə xidmət edir.

23. Fərqanə Abdullayeva

Virtual məkanda milli maraqlara ziyanlı kontentlərlə mübarizə mexanizmləri və texnologiyaları

ETN İnformasiya Texnologiyaları İnstitutu

Dezinformasiya, manipulyativ media materialları və süni intellekt əsaslı deepfake texnologiyaları milli təhlükəsizlik maraqlarına birbaşa təsir göstərir. Bu səbəbdən belə kontentlərin vaxtında aşkarlanması və qarşısının alınması üçün effektiv mexanizm və texnologiyaların tətbiqi mühüm əhəmiyyət kəsb edir. Tədqiqat işində ziyanlı kontentlərlə mübarizədə tətbiq olunan hüquqi, institusional və texnoloji mexanizmlər kompleks şəkildə araşdırılmışdır. Süni intellekt əsaslı kontent analizi, deepfake aşkarlanması, avtomatik monitorinq sistemləri, həmçinin AI Act və ENISA, NIST, ISO beynəlxalq standartları əsasında risklərin idarə olunması və kibermüdafiə yanaşmaları təhlil edilmişdir.

24. Səid Məmmədov

Dezinformasiyanın dövlətin kibersuverenliyinə təsirinin ölçülməsi və qiymətləndirilməsi

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat işində dezinformasiya ekosisteminin milli kibersuverenliyə yaratdığı strateji təhdidlər araşdırılır və onların analitik qiymətləndirilməsi metodları analiz olunur. ABŞ, Avropa Birliyi ölkələri, Rusiya və Çin kimi dövlətlərin suverenlik modellərinin xüsusiyyətləri müqayisə edilir, süni intellekt və "deepfake" texnologiyalarının manipulyasiya imkanları araşdırılır. Tədqiqat işində dezinformasiyanın təsirini ölçmək məqsədilə məlumat axını, cəmiyyətə təsir və suverenlik nəticələri üzrə indikatorları əhatə edən üçsəviyyəli qiymətləndirmə arxitekturası təsvir olunur. Strateji risklərin idarə olunması üçün texniki, institusional və sosial aspektləri inteqrasiya edən çoxmeyarlı təhdid qiymətləndirmə modelinin tətbiqinin zəruriliyi vurğulanır.

25. Babək Nəbiyev, Könül Daşdəmirova

Kibersuverenliyin təmin olunması üçün milli kibertəhlükəsizlik sisteminin formalaşması mexanizmlərinin işlənməsi

ETN İnformasiya Texnologiyaları İnstitutu

Elektron dövlət mühitində informasiya-kommunikasiya texnologiyalarından geniş istifadə edilməsi, eləcə də milli təhlükəsizliyi təşkil edən bütün sahələrin kiberməkana inteqrasiyası informasiya təhlükəsizliyi problemlərinin aktuallaşmasına səbəb olmuşdur. Tədqiqatda kibermühitdə informasiya təhlükəsizliyinin milli təhlükəsizliyin və kibersuverenliyin təmin olunması üçün əsas komponentlərdən birinə çevrilməsi ön plana çəkilmişdir. Qlobal mühitdə kibersuverenliyi təmin etmək və milli kiberməkan üzərində effektiv nəzarəti həyata keçirmək üçün Milli Kibertəhlükəsizlik Sistemlərinin yaradılması təklif edilmişdir.

26. Tamilla Bayramova

Dövlətin kibersuverenliyinin təmin edilməsi üçün milli proqram mühəndisliyinin formalaşması problemləri

ETN İnformasiya Texnologiyaları İnstitutu

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.

27. Aidə Mustafayeva

Rəqəmsal dövlət xidmətlərində data və bulud suverenliyinin təmin olunması üçün metodik yanaşmalar

Mingəçevir Dövlət Universiteti

Qlobal rəqəmsal transformasiya dövlət idarəçiliyində struktur dəyişikliklərini və informasiya resurslarının sürətli artımını şərtləndirmişdir. Elektron hökumət, bulud texnologiyaları və süni intellektin tətbiqi xidmətlərin səmərəliliyini artırsa da, məlumat təhlükəsizliyi və suverenliyi sahəsində yeni çağırışlar yaradır. Tədqiqatlar göstərir ki, hüquqi boşluqlar, texnoloji asılılıq, institusional çatışmazlıqlar və kadr potensialının yetərsizliyi data və bulud suverenliyini risk altına qoyur. Suveren bulud infrastrukturunun yaradılması, məlumatların lokallaşdırılması, kriptoqrafik protokollar, normativ gücləndirmə və kadr hazırlığı kompleks yanaşma olaraq bu risklərin minimuma endirilməsini təmin edir və dövlətin kibersuverenliyini gücləndirir.

28. Ayna Əlixanova

Kibersuverenlik konsepsiyası və onun dövlət təhlükəsizliyi sistemində rolu

"Magen David Women in Azerbaijan" təşkilatı

Tədqiqat işində müasir rəqəmsallaşma şəraitində kibersuverenlik konsepsiyası və onun dövlət təhlükəsizlik sistemində rolu təhlil olunur. İşdə kibersuverenliyin normativ, texnoloji, informasiya və iqtisadi komponentləri analiz olunur, həmçinin beynəlxalq hüquqi mühitdə vahid yanaşmanın olmaması, terminoloji qeyri-müəyyənlik, texnoloji asılılıq və insan hüquqları ilə təhlükəsizlik arasında balans kimi problemlər göstərilir. Azərbaycan təcrübəsində kibertəhlükəsizlik sahəsində formalaşmış institusional mexanizmlər və milli prioritetlər nəzərdən keçirilir. Kibersuverenliyin təmin edilməsi üçün hüquqi bazanın təkmilləşdirilməsi, yerli texnologiyaların inkişafı, kadr hazırlığı və beynəlxalq əməkdaşlığın gücləndirilməsi istiqamətində məqsədyönlü fəaliyyətin həyata keçirilməsinin vacibliyi vurğulanır.

29. **Banovsha Abbasova, Tabriz Jafarov**

The transformation of state sovereignty in the digital age: theoretical and practical challenges of cyber sovereignty

ADA University

This study examines cyber sovereignty as a challenge to traditional conceptions of state sovereignty grounded in territorial authority. It argues that cyber sovereignty should be understood as a dynamic and hybrid concept shaped by legal norms, technological architecture, and institutional practices. The analysis addresses key practical problems, including transboundary jurisdiction, attribution of cyber operations, and tensions between security measures and rights, with particular reference to Yahoo! Inc. v. LICRA. It further evaluates national and international responses, concluding that existing frameworks enhance coordination but remain constrained by structural features of cyberspace.

II SEKSİYA

DÖVLƏTİN KİBERSUVERENLİYİNİN TƏMİN OLUNMASININ ELMİ SİYASİ-HÜQUQİ VƏ TƏŞKİLATİ ASPEKTLƏRİ

Kiçik konfrans zalı, saat 14:00–17:30

Həmsədrlər: **AMEA-nın müxbir üzvü Məsumə Məmmədova, texnika elmləri üzrə fəlsəfə doktoru Ziyafət Əmirov**

Elmi katib: **texnika elmləri üzrə fəlsəfə doktoru Ramiz Şıxəliyev**

1. **Elvin Balacanov**

   Kibersuverenlik kontekstində kritik informasiya infrastrukturunun təhlükəsizliyi: Azərbaycan Respublikasının normativ və strateji yanaşması

   Dövlət Təhlükəsizliyi Xidməti, Milli kibermərkəz

   Kritik informasiya infrastrukturunun (Kİİ) təhlükəsizliyi dövlətin milli kiberməkan üzərində effektiv nəzarət imkanlarının formalaşmasında əsas faktorlardan biri kimi çıxış edir. Son illər ərzində Kİİ təhlükəsizliyinin təmin edilməsi məqsədilə hüquqi, təşkilati və texniki-texnoloji sferalarda mühüm addımlar atılmış, müvafiq normativ baza və institusional mexanizmlər formalaşdırılmışdır. Bununla yanaşı, Kİİ subyektləri tərəfindən infrastrukturun təhlükəsizliyinə daha çox önəm verilməsinə və risk əsaslı yanaşmanın dərinləşdirilməsinə zərurət yaranmışdır. Tədqiqat işində mövcud yanaşmalar təhlil edilir, qarşıda duran çağırışlar müəyyənləşdirilir və kibersuverenliyin praktiki təminat mexanizmi kimi Kİİ təhlükəsizliyinin gücləndirilməsi üzrə inkişaf istiqamətləri irəli sürülür.

2. **Ziyafət Əmirov**

   Süni intellekt əsaslı dezinformasiyanın yaradılması, tətbiqi və onunla mübarizə

   DTX-nin Heydər Əliyev adına Akademiyası

   Müasir dövrün qlobal informasiya müharibələri kontekstində saxta məlumatların və xəbərlərin yayılması ictimai şüurun

manipulyasiyası üçün əsas vasitələrdən birinə çevrilmişdir. Tədqiqat işində saxta xəbər (deepfake), süni intellekt agenti anlayışları, habelə süni intellekt əsaslı dezinformasiyanın yaradılması mexanizmləri, onun kibertəhlükəsizlik mühitində tətbiqi və yaratdığı risklər təhlil edilir. Dərin öyrənmə modelləri, generativ neyron şəbəkələr və avtomatlaşdırılmış botlar vasitəsilə saxta məzmunun sürətli yayılması izah olunur. Eyni zamanda, dezinformasiyanın aşkarlanması üçün istifadə olunan texniki və təşkilati müdafiə yanaşmaları, media savadlılığı və hüquqi tənzimləmələrin rolu şərh edilir.

3. **Rəşad Əliyev, Sərfi Həbibova, Ülviyyə Məmmədova**

Təhlükəsizlik əməliyyatları mərkəzləri üçün real vaxt hücum vizuallaşdırma sisteminin dizaynı

Xəzər Universiteti, YER xSP MMC

Təşkilatların infrastrukturlarını hədəf alan kiberhücumlar həm miqyas, həm də mürəkkəblik baxımından artaraq vəziyyət barədə effektiv məlumatlılıq mexanizmlərinə artan tələbat yaradır. Təhlükəsizlik Məlumatı və Hadisə İdarəetmə (SIEM) sistemləri təhlükəsizlik hadisələrinin mərkəzləşdirilmiş aşkarlanmasına və təhlilinə imkan versə də, onların vizuallaşdırma imkanları əsasən mətn və idarəetmə panelinə əsaslanan təsvirlərlə məhdudlaşır. Mövcud qlobal kibertəhdid xəritələri yüksək səviyyəli anlayışlar təqdim edir, lakin təşkilata xas aktuallığa malik deyil. Tədqiqat işində təhlükəsizlik xəbərdarlıqlarını (*alert*-ləri) coğrafi kibertəhlükə xəritəsinə çevirən real vaxt rejimində SIEM-ə əsaslanan təhlükələrin vizuallaşdırılması üçün yanaşma təklif olunur.

4. **Şakir Mehdiyev, Nəzrin Rzayeva**

Dövlətin kibersuverenliyi və enerji təhlükəsizliyinə yeni tələblər

ETN İnformasiya Texnologiyaları İnstitutu

İnformasiya-kommunikasiya texnologiyalarının enerji sektorunda geniş tətbiqi bu sahəni kiberhücumlara qarşı daha həssas etmişdir. Bu baxımdan dövlətlərin rəqəmsal məkan üzərində suverenliyinin gücləndirilməsi strateji zərurət kimi çıxış edir. Tədqiqat işində

kiberməkan üzərində dövlət nəzarətinin hüquqi, institusional və texnoloji aspektləri təhlil edilir, kritik enerji sistemlərinin qorunmasında kiberstrategiyaların rolu qiymətləndirilir. Kibersuverenliyin gücləndirilməsi yalnız milli təhlükəsizlik üçün deyil, həm də enerji sektorunun dayanıqlı inkişafı və beynəlxalq rəqabət qabiliyyətinin artırılması üçün kritik əhəmiyyət kəsb edir.

5. **Ülkər Əlizadə**

Mürəkkəb təsvirlərin tanınması: proqram paketi, arxitektura və praktik tətbiqlər

DTX-nin Heydər Əliyev adına Akademiyası

Tədqiqat işində mürəkkəb struktura malik təsvirlərin tanınması üçün adaptiv, mərhələli emal sistemi təqdim olunur. Səs-küy, qeyri-bərabər işıqlandırma və natamam konturlar şəraitində sistemin dayanıqlılığını artırmaq üçün Qaus filtrasiyası, Canny sərhəd aşkarlanması və riyazi morfologiya əməliyyatlarının kombinasiyası tətbiq edilmişdir. Tanınma mərhələsində KNN alqoritmindən istifadə olunmuş və nəticələrin keyfiyyətinə uyğun olaraq parametrlərin avtomatik tənzimlənməsi mexanizmi qurulmuşdur. İterativ emal mexanizmi parametrlərin adaptiv dəyişdirilməsi yolu ilə tanınma nəticələrinin stabilliyini artırır. Aparılan eksperimental sınaqlar təklif olunan yanaşmanın həm biometrik, həm də tibbi diaqnostik görüntülərdə yüksək adaptivlik nümayiş etdirdiyini göstərir.

6. **Akif Orucəliyev, Fərid Süleymanov**

İnformasiya təhlükəsizliyi ixtisası üzrə kadr hazırlığının mövcud vəziyyəti və bəzi problemləri

DTX-nin Heydər Əliyev adına Akademiyası

İnformasiya təhlükəsizliyi ixtisası üzrə bakalavr hazırlığı üçün nəzərdə tutulmuş təhsil proqramında yer alan humanitar, ixtisas, eləcə də seçməfənlərinin bu ixtisas üzrə mütəxəssis hazırlığında real vəziyyətin araşdırılmasına ehtiyac vardır. Tədqiqat işində "İnformasiya təhlükəsizliyi" ixtisası üzrə təhsil verən ali məktəblərin tədris planlarında yer alan ixtisas və humanitar fənlərinin mövcud tədrisinin bəzi aspektləri araşdırılır, daha savadlı

kadr hazırlığı üçün Azərbaycan Respublikasının müvafiq strategiya və tədbirləri əsasında nəyə daha çox diqqət yetirilməli olan məsələlər analiz edilir.

7. **Nigar Məmmədova**

İnersial naviqasiya sistemlərində sensor siqnallarının zaman sıraları şəklində toplanmasının texnoloji suverenlik kontekstində texniki və riyazi əsaslandırılması

DTX-nin Heydər Əliyev adına Akademiyası

Tədqiqat işində inersial naviqasiya sistemlərində istifadə olunan akselerometr və giroskop sensorlarından əldə edilən ölçmə siqnallarının diskret zaman oxu üzrə zaman sıraları formasında toplanmasının texniki və riyazi əsasları araşdırılmışdır. MEMS əsaslı sensorların sabit nümunələmə tezliyi ilə işləməsi, ölçmələrin vahid zaman indeksi üzrə sinxronlaşdırılması və vahid ölçmə vektoru şəklində təqdim edilməsi modelləşdirilmiş laboratoriya nümunələri əsasında təhlil olunmuşdur. Sensor siqnallarının fiziki uyğunluğu, səs-küy təsiri və statistik xarakteristikaları zaman sıraları modeli ilə qiymətləndirilmişdir. Alınan nəticələr peyk sistemlərindən asılı olmayan naviqasiya həlləri vasitəsilə avtonom sistemlərdə texnoloji suverenliyin təmin olunmasına töhfə verir.

8. **Rəşad Rəsulzadə**

Süni intellekt əsaslı kibertəhlükəsizlik mexanizmləri və milli kibersuverenlik

DTX-nin Heydər Əliyev adına Akademiyası

Tədqiqat işində süni intellekt əsaslı kibertəhlükəsizlik mexanizmlərinin mahiyyəti, onların dövlət səviyyəsində tətbiq imkanları və milli informasiya resurslarının qorunmasında rolu təhlil olunur. Maşın öyrənməsi və dərin öyrənmə alqoritmləri əsasında kiberhücumların erkən aşkarlanması, anomaliyaların müəyyən edilməsi və təhlükələrin proqnozlaşdırılması imkanları araşdırılır. Eyni zamanda, süni intellekt texnologiyalarının tətbiqi zamanı yaranan elmi-praktiki problemlər, o cümlədən, yerli məlumat bazalarının çatışmazlığı, xarici texnoloji asılılıq məsələləri

araşdırılır. Dövlət səviyyəsində süni intellekt texnologiyalarının təhlükəsiz və davamlı tətbiqi üçün tövsiyələr irəli sürülür.

9. Fərid Qasımlı, Yadigar İmamverdiyev

Enerji sektorunda adaptiv kibertəhlükəsizlik: dinamik risk modelləri

Azərbaycan Texniki Universiteti

Tədqiqat işində enerji sektorunda kibertəhlükəsizlik problemləri sistemli şəkildə təhlil edilmiş, hücumların mərhələli inkişafını modelləşdirmək üçün Markov zənciri əsasında dinamik vəziyyət modeli qurulmuş və qeyri-müəyyənlik şəraitində riskin qiymətləndirilməsi üçün Bayesian risk çərçivəsi təklif edilmişdir. Təklif olunan inteqrə olunmuş Markov–Bayesian yanaşma riskin zaman üzrə dəyişməsini və posterior ehtimalların yenilənməsini nəzərə alaraq daha dəqiq təhlükə qiymətləndirməsinə imkan verir. Tədqiqat nəticələri göstərir ki, adaptiv və riyazi əsaslandırılmış təhlükəsizlik modelləri enerji infrastrukturunda dayanıqlığın artırılmasına və strateji qərarların optimallaşdırılmasına əhəmiyyətli töhfə verir.

10. Vüqar Hüseynli

Dinamik proqramlaşdırma və qərar ağaclarının yanaşması ilə izaholunan süni intellekt agenti

DTX-nin Heydər Əliyev adına Akademiyası

Süni intellekt (Sİ) sistemləri mürəkkəb qərarvermə, optimallaşdırma və vəziyyətlərarası keçid problemlərinin həllinə əsaslanır. Bu problemlərin böyük əksəriyyəti dinamik proqramlaşdırma (DP), ağac və qraf strukturlarının birgə istifadəsini tələb edir. Tədqiqat işində DP-nin optimal qərarların saxlanması və yenidən istifadəsindəki rolu, ağacların qərar ardıcıllığını formalaşdırmaq funksiyası və qraf strukturlarının vəziyyət məkanını modelləşdirmədəki əhəmiyyəti sistemli şəkildə araşdırılır. Bundan əlavə, heç bir xarici kitabxanaya ehtiyac olmadan DP, ağac və qraf strukturlarına əsaslanan Sİ alqoritmi və onun riyazi modeli təqdim olunur.

11. Əfruz Qurbanova, Mehriban Bağırova

Virtual məkanda dövlətin linqvistik suverenliyi: dilin ekosistemi, problemlər və həlli yolları

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat işində rəqəmsal ekosistem kontekstində dillərin funksional müstəqilliyi və dayanıqlılığı analiz olunur, linqvistik suverenliyin əsas aspektləri müəyyən edilir. Rəqəmsal mühitdə linqvistik suverenliyin təmini və inkişafı üzrə konseptual yanaşmalar təhlil olunur, bu müstəvidə linqvistik suverenliyin çoxsəviyyəli modeli təklif edilir. Virtual məkanda linqvistik suverenliyə olan əsas təhdidlər müəyyən edilir və onların aradan qaldırılması üçün milli dil ekosisteminin formalaşdırılması zəruriyyəti göstərilir. Rəqəmsal dövlət platformasında dil ekosisteminin formalaşması imkanları və əsas komponentləri müəyyənləşdirilir. Milli dillərin rəqəmsal məkanda funksional imkanlarının genişləndirilməsi və rəqəmsal suverenliyinin təmin olunması istiqamətində tövsiyələr verilir.

12. Rauf İsmayılzadə

Kiberdayanıqlılıq konsepsiyası və onun kibersuverenliyin təmin olunmasında rolu

DTX-nin Heydər Əliyev adına Akademiyası

Tədqiqat işində kibertəhlükəsizlik və kibermüdafiə arasındakı qarşılıqlı əlaqə araşdırılır və kiberdayanıqlılığa dair yanaşmalar analiz edilir. İşdə kiberdayanıqlılığın təmin olunması üçün yeni konseptual yanaşma təqdim olunur. Təklif olunan konseptual model artan kibertəhdidlər fonunda kibertəhlükəsizlik və kibermüdafiənin dayanıqlılığını gücləndirmək üçün zəruri olan taktika və tədbirləri müqayisəli analiz edir. İşdə CRRT və MACS-in tarixi, məqsədləri və gələcək inkişaf istiqamətləri araşdırılır. Avropa Birliyi səviyyəsində innovasiya siyasəti çərçivəsində daim dəyişən təhdid mühitinə qarşı dayanıqlı və koordinasiyalı müdafiə imkanlarının formalaşdırılması məsələləri təhlil edilir.

13. **Kamran Xəlilov**

Kibertəhlükəsizliyin təmin edilməsində cinayət-hüquqi vasitələrin rolu və rəqəmsal dayanıqlılığın qorunması

Bakı Dövlət Universiteti, DTX-nin Heydər Əliyev adına Akademiyası

Bu tədqiqat işində kibertəhlükəsizliyin təmin edilməsində cinayət hüquqi mexanizmlərin rolu təhlil edilir. Rəqəmsal sübutun dəyişdirilə bilən xarakteri, transsərhəd yerləşməsi və texnoloji mürəkkəbliyi istintaq və məhkəmə mərhələsində xüsusi prosessual təminatların tətbiqini zəruri edir. Tədqiqat normativ və doktrinal təhlil əsasında göstərir ki, əməlin yalnız cinayət məsuliyyəti yaradan hüquq pozuntusu kimi müəyyən edilməsi kifayət deyil. Sübutların qanuni qaydada əldə olunması, qorunması və məhkəmədə etibarlı qiymətləndirilməsi hüquqi reaksiyanın effektivliyini müəyyən edən əsas amillərdir. Rəqəmsal dayanıqlılıq texniki müdafiə tədbirləri ilə yanaşı, hüquqi sabitlik, beynəlxalq əməkdaşlıq, effektiv və balanslı cinayət-prosessual mexanizmlərin tətbiqindən asılıdır.

14. **Aqşin Paşayev, Səməd Dursunov**

Darknet və Dark web infrastrukturunun dövlətin kibersuverenliyinə yaratdığı risklər və təhdidlər

ETN İnformasiya Texnologiyaları İnstitutu

İnternetin sərhədsiz və paylanmış texniki arxitekturası informasiyanın milli sərhədlərdən kənara sürətlə ötürülməsinə imkan yaradır ki, bu da ənənəvi dövlət nəzarət mexanizmlərinin effektivliyini azaldır. Tədqiqat işində internet mühitini Surface Net, Deep Net və DarkNet səviyyələrində təhlil edir və kibersuverenliyə təsirini araşdırır. Araşdırma nəticələri göstərir ki, bu texnoloji xüsusiyyətlər hüquqi tənzimləməni mürəkkəbləşdirir, informasiya təhlükəsizliyi baxımından dezinformasiya, manipulyasiya, kiberhücum və kibertəhdid risklərinin artmasına səbəb olur. Nəticə etibarilə, kibersuverenlik problemi hüquqi, texnoloji və beynəlxalq əməkdaşlıq çərçivəsində kompleks yanaşma olaraq baxılmasını tələb edir.

15. **Rəsmiyyə Mahmudova**

Əhalinin rəqəmsal savadlılıq səviyyəsinin dövlətin kibersuverenliyinə təsirinin araşdırılması və təhlili

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat işində əhalinin rəqəmsal savadlılıq səviyyəsi ilə dövlətin kibersuverenliyi arasındakı qarşılıqlı əlaqə araşdırılır. Müasir dövrdə kibersuverenlik təkcə infrastrukturun qorunması deyil, həm də vətəndaşların kiberməkandakı davranışlarından birbaşa asılıdır. İşdə rəqəmsal savadlılığın aşağı olmasının sosial mühəndislik hücumlarına, dezinformasiya kampaniyalarına və fərdi məlumatların sızmasına şərait yaradaraq dövlətin rəqəmsal sərhədlərini necə zəiflətdiyi analiz edilir. Tədqiqatın nəticələri göstərir ki, kibersavadlı cəmiyyət dövlətin kibermüdafiə sisteminin "insan layını" təşkil edərək milli təhlükəsizliyin ayrılmaz hissəsinə çevrilir. Sonda əhalinin rəqəmsal bacarıqlarının artırılması vasitəsilə milli kiberdayanıqlılığın gücləndirilməsi üçün strateji tövsiyələr verilir.

16. **Bikəs Ağayev, Şakir Mehdiyev, Lalə Əliyeva**

Xidməti danışıqların kriptoqrafik təminatı məsələləri dövlət kibersuverenliyi kontekstində

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat işində "Dövlət kibersuverenliyi", "Texnoloji suverenlik", "İnformasiya təhlükəsizliyi", "Kibertəhlükəsizlik" və s. kimi əlaqəli anlayışlar araşdırılır və müqayisəli analizi aparılır. Aparılan tədqiqatlar göstərir ki, müxtəlif dərəcəli məxfi və dövlət sirri daşıyan məlumatlar, mühüm dövlət orqanlarının, təşkilatların xidməti danışıqları çoxsəviyyəli struktura malik olan dövlət kibersuverenliyi və texnoloji suverenlik məsələlərinin tərkib hissələrindən biri hesab edilə bilər. Bu yanaşmaya əsasən otaq şəraitində aparılan müəyyən məxfiliyə malik xidməti danışıqların iştirakçılar tərəfindən gizli yazılması və otaqdan kənara sızan vibroakustik siqnallar vasitəsilə məlumatların əldə edilməsinə qarşı mühafizə məsələlərinə baxılır və təkliflər verilir.

17. **Kəmalə Həşimova**

Virtual məkanda fövqəladə halların dövlətin kibersuverenliyinə təsirlərinin analizi və perspektiv vəzifələr

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat işində müasir geosiyasi şəraitdə fövqəladə halların (təbii fəlakətlər, hərbi münaqişələr, texnogen qəzalar və s.) dövlətin rəqəmsal sərhədlərinə və idarəetmə mexanizmlərinə təsiri kompleks şəkildə təhlil olunur. İşdə rəqəmsallaşmanın dövlət suverenliyinin ayrılmaz tərkib hissəsinə çevrildiyi vurğulanır və böhran vəziyyətində yaranan virtual risklərin milli təhlükəsizliyə yaratdığı təhdidlər araşdırılır. Fövqəladə hallar zamanı virtual məkanda yaranan risklər kompleks şəkildə təsnif edilmiş, onların dövlət idarəçiliyinə təsiri analiz olunmuşdur. Tədqiqat işində virtual məkanda yaranan hibrid təhdidlərə qarşı dövlətin rəqəmsal dayanıqlılığını təmin edən "Kibersəfərbərlik" konseptual modeli təklif edilir.

18. **Rəsmiyyə Mahmudova, Çinarə İsayeva**

Rəqəmsal fərqlərin dövlətin kibersuverenliyinə yaratdığı təhlükələr və risklərin analizi

ETN İnformasiya Texnologiyaları İnstitutu

Rəqəmsal fərqlərin artması dövlətlərin kibersuverenliyinə fundamental təhdid yaradan amil kimi çıxış edir. İnfrastruktur, texnologiya və fərdi rəqəmsal bacarıqlardakı bərabərsizliklər kiberhücumlara qarşı milli müdafiə sistemlərini zəiflədir, milli təhlükəsizlik və iqtisadi sabitlik üçün risklər yaradır. Bu fərqlər dövlətlərin öz rəqəmsal ekosistemlərini müstəqil idarə etmə imkanlarını məhdudlaşdırır, xarici texnoloji asılılığı dərinləşdirir və informasiya müharibələrində strateji zəifliklər doğurur. Tədqiqat işində rəqəmsal uçurumun kibersuverenlik kontekstində yaratdığı təhlükələrin analizi aparılır və rəqəmsal bərabərsizliyin aradan qaldırılması vasitəsilə milli kiberdayanıqlılığın artırılması üçün konseptual strateji yanaşmalar təhlil olunur.

19. **Sübhan Qaragözov**

Rəqəmsal transformasiya şəraitində layihələrin idarə olunmasında süni intellekt texnologiyalarının tətbiqi: kibertəhlükəsizlik və rəqəmsal dayanıqlılıq çağırışları

Azərbaycan Memarlıq və İnşaat Universiteti

Rəqəmsal transformasiya layihələrin idarə olunması proseslərinə əhəmiyyətli təsir göstərmiş və süni intellekt texnologiyalarının qərarvermə, risklərin proqnozlaşdırılması və performansın optimallaşdırılması məqsədilə geniş tətbiqinə şərait yaratmışdır. Süni intellekt əsaslı yanaşmalar layihələrin səmərəliliyini artırsa da, eyni zamanda kibertəhlükəsizlik riskləri və rəqəmsal dayanıqlılıqla bağlı yeni çağırışlar formalaşdırır. Tədqiqat işində rəqəmsal transformasiya şəraitində layihələrin idarə olunmasında süni intellekt texnologiyalarının tətbiqi kibertəhlükəsizlik və rəqəmsal dayanıqlılıq kontekstində araşdırılır. Tədqiqat çərçivəsində məlumatların təhlükəsizliyi, sistemlərin etibarlılığı və təşkilati hazırlıq məsələləri təhlil edilir, həmçinin əldə olunan nəticələrin elmi və praktiki əhəmiyyəti göstərilir.

20. **Rahib Aghababayev**

Inventory-level triage for android logical images: automated artifact type classification

Azerbaijan Technical University

This study examines how accurately artifacts can be automatically identified and classified by type within an Android OS version 15 logical image. We propose a lightweight triage pipeline that derives features from file metadata, MIME/type hints, and path context, then applies supervised learning to assign coarse artifact type as Image, Audio, Document, Log/Config, App Cache/Object. To avoid duplicate leakage, evaluation uses a SHA-256 grouped split on 348 labeled files. On the leakage-aware test set, Logistic Regression and Random Forest achieve macro-F1=0.5808 and weighted-F1=0.9706, outperforming a rule-based baseline macro-F1=0.2496.

21. Xumar Şirəliyeva, İnci Abdullayeva

IIoT təhlükəsizliyi kibersuverenliyin dayağı kimi

Azərbaycan Texniki Universiteti

Industrial IoT (IIoT) təhlükəsizliyi kibers**u**verenliyin kritik komponentlərindən biridir**.** fiziki proseslərin etibarlılığını, strateji əhəmiyyət daşıyan verilənlərin təhlükəsizliyinə nəzarəti və sənaye əməliyyatlarının davamlılığını təmin edir. Sənaye idarəetmə sistemlərinin və əməliyyat texnologiyalarının rəqəmsal şəbəkələrə inteqrasiyası hücum səthini genişləndirərək dövlətlər və təşkilatlar üçün yeni risklər yaradır. Tədqiqat işində IIoT sistemində yaranan texnoloji asılılıqlar, kiberrisklər, məlumat suverenliyi problemləri analiz olunur, həmçinin təhlükəsizliyin gücləndirilməsi üçün yanaşmalar təklif olunur. Nəticədə IIoT təhlükəsizliyi sadəcə texniki məsələ deyil, eyni zamanda milli təhlükəsizlik və iqtisadi dayanıqlılıq konteksində strateji prioritet kimi əsaslandırılır.

22. Məkrufə Hacırəhimova

Dövlətin kibersuverenliyində intellektual potensialın rolunun təhlili və qiymətləndirilməsi

ETN İnformasiya Texnologiyaları İnstitutu

Rəqəmsal transformasiya dövründə qlobal miqyasda kiberhücumların artması dövlətlərin kibersuverenliyinin təmin olunmasında intellektual potensialın rolunu ön plana çıxarmışdır. Tədqiqatlar göstərir ki, intellektual potensial dövlətin kibersuverenliyinin strateji dayağı kimi qiymətləndirilməkdədir. Tədqiqat işində dövlətin kibersuverenliyinin formalaşmasında və qorunmasında intellektual potensialın rolu araşdırılır. Azərbaycanda kibertəhlükəsizlik üzrə kadr potensialının mövcud vəziyyəti təhlil olunur, bu sahədəki problemlər və inkişaf etmiş ölkələrin əmək bazarında ən çox tələb olunan peşələr analiz edilir. Dövlətin kibersuverenliyində intellektual potensialın rolunu qiymətləndirmək üçün model təklif olunur.

23. Oqtay Ələkbərov

Kibervalyutalar və dövlətin rəqəmsal suverenliyi: mövcud vəziyyəti, təhlükəsizlik məsələləri və risklər

ETN İnformasiya Texnologiyaları İnstitutu

Kibervalyutaların sürətli yayılması dövlətlərin maliyyə və rəqəmsal suverenliyi üçün yeni risklər yaratmışdır. Mərkəzləşdirilməmiş xarakterə malik bu valyutalar pul siyasətinə nəzarəti zəiflədə, maliyyə sabitliyinə təsir göstərə və qanunsuz əməliyyatların artmasına şərait yarada bilər. Tədqiqat işində kibervalyutaların dövlət suverenliyinə təsiri, kibertəhlükəsizlik problemləri, anonimlik və maliyyə riskləri təhlil olunur. Eyni zamanda, dövlətlərin tənzimləmə tədbirləri kimi alternativ yanaşmalar nəzərdən keçirilir.

24. Məmməd Məmmədov

Türk dövlətlərinin ortaq buludu: rəqəmsal suverenlik və təhlükəsizlik

Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyası

Tədqiqat işində rəqəmsal suverenliyin təmin olunması üçün Türk dövlətlərinin ortaq bulud platformasının yaradılmasının konseptual əsasları araşdırılır. Dövlətlərin informasiya və data üzərində nəzarətinin yalnız kibertəhlükəsizlik yox, eyni zamanda siyasi və iqtisadi müstəqillik məsələsi olduğu qeyd olunur. İşdə Türk Dövlətləri Təşkilatı çərçivəsində ortaq rəqəmsal bulud infrastrukturunun yaradılması təklif olunur. Bu infrastrukturun yaradılması üzv dövlətlərə məlumatlarını milli və regional səviyyədə təhlükəsiz idarə etmək imkanı yaradacaqdır.

25. Cəlal Mehdiyev, Vüsal Şahbazov

AzClaims: Azərbaycan dilində iddia çıxarımı üçün verilənlər toplusu

Azərbaycan Texniki Universiteti,

ETN İnformasiya Texnologiyaları İnstitutu

Müasir informasiya mühitində dezinformasiyanın yayılması ictimai rəyin manipulyasiyasına və dövlət institutlarına inamın sarsıdılmasına səbəb olur. Fakt yoxlama informasiya təhlükəsizliyi və dövlət kibersuverenliyinin təmin edilməsində mühüm rol

oynayır. Lakin böyükhəcmli mətnlərdən iddiaların avtomatik çıxarılması, xüsusilə Azərbaycan dili üçün aktual problemdir. Bu məqalədə Azərbaycan dilində iddia çıxarımı üçün yeni AzClaims verilənlər toplusu təqdim olunur. Standart çoxdilli transformer modelləri AzClaims üzərində sınaqdan keçirilmiş və Azərbaycan dilinin xüsusiyyətləri nəzərə alınmaqla təkmilləşdirmişdir.

26. İradə Ələkbərova

Multikriterial sosial kredit mexanizmlərinin kibersuverenliyin qiymətləndirilməsində tətbiqi məsələləri

ETN İnformasiya Texnologiyaları İnstitutu

Tədqiqat sosial kreditləşmənin kibersuverenliklə inteqrasiyasının potensial üstünlüklərini araşdırır və bu inteqrasiyanın yarada biləcəyi riskləri müəyyənləşdirir. Tədqiqatda əsas məqsəd, kibersuverenliyini gücləndirmək məqsədi ilə sosial kredit sistemini tətbiq edən dövlətin əldə edəcəyi perspektivləri və riskləri müəyyən etməkdir. Tədqiqatın əsas yeniliyi kibersuverenliyin qiymətləndirilməsi üçün multikriterial sosial kredit modelinin təklif edilməsidir. Bu model vasitəsilə verilənlərin suverenliyi, texnoloji asılılıq və hüquqi uyğunluq faktorlarının ümumi kiberdayanıqlığa təsiri analiz olunur.

27. Firudin Ağayev, Gülarə Məmmədova, Rəna Məlikova, Lalə Zeynalova

Böyük verilənlər əsasında təhsil ekosistemi üzrə data suverenliyinin qorunması problemləri

ETN İnformasiya Texnologiyaları İnstitutu

Rəqəmsal transformasiyalar və qloballaşma kontekstində təhsil sistemi keyfiyyəti artırmaq və idarəetmə proseslərini optimallaşdırmaq zərurəti ilə üzləşir. Təhsil prosesləri getdikcə rəqəmsal platformalar, bulud xidmətləri və böyük verilənlərin analitikası vasitəsilə həyata keçirilir. Belə ki, təhsil sisteminin rəqəmsal transformasiyası şəraitində data suverenliyi milli rəqəmsal təhlükəsizliyin əsas komponentlərindən birinə çevrilmişdir. Tədqiqat işində böyük verilənlər əsasında təhsil ekosisteminin yaradılması və inkişafında məlumatların qorunması

mexanizmlərinin nəzəri, hüquqi və praktik aspektləri təhlil edilib. Bununla yanaşı, distant təhsil prosesində süni intellektdən istifadə ilə bağlı çətinliklər, etik və təhlükəsizlik məsələləri araşdırılır.

28. Вагиф Мамедалиев

Киберсуверенитет в медицине 4.0: многоуровневая модель контроля и подотчётности

Институт Информационных Технологий МНО

В работе под понятием киберсуверенитета в медицине 4.0 подразумевается операционная способность, выходящая за рамки суверенитета данных и кибербезопасности, и интегрирующая управленческие, технические, интероперабельные и доказательные механизмы подотчётности в распределённых цифровых системах здравоохранения. Предложена четырёхуровневая модель поддержки киберсуверенитета в среде медицины 4.0. Модель связывает принципы киберсуверенитета с конкретными исполнимыми целями контроля и требованиями к доказательствам, охватывающими распространение и отзыв согласия, отслеживание источников данных, обязательства поставщиков, переносимость и непрерывную валидацию механизмов контроля.

29. Xəyyam Nurəliyev

Kibermüdafiə strategiyası: problemlər, konseptual baxışlar və formalaşma mexanizmləri

ETN İnformasiya Texnologiyaları İnstitutu

İnformasiya texnologiyalarının sürətli inkişafı kibertəhdidlərin sayını və təsir dairəsini əhəmiyyətli dərəcədə genişləndirmişdir. Tədqiqat nəticələri göstərir ki, kibermüdafiə yalnız texnoloji tədbirlərlə məhdudlaşmamalı, həmçinin normativ-hüquqi baza, beynəlxalq əməkdaşlıq, insan resurslarının inkişafı və risklərin idarə olunmasını da əhatə etməlidir. Kibermüdafiə mövcud risklərin düzgün qiymətləndirilməsi, konseptual yanaşmaların sistemli şəkildə formalaşdırılması və tətbiq mexanizmlərinin dəqiq müəyyən olunmasından birbaşa asılıdır. Tədqiqat nəticəsində müasir kibermüdafiə texnologiyalarının problemləri, mexanizmləri tədqiq edilmiş və yeni konseptual yanaşma təklif olunmuşdur.

KONFRANSIN BAĞLANIŞI

Böyük konfrans zalı, saat: 17:30-18:00

Sədr: **akademik Rasim Əliquliyev**

Elmi katib: **texnika elmləri üzrə fəlsəfə doktoru Fərhad Yusifov**

Konfransın qərar layihəsinin müzakirəsi