oynayır. Lakin, dinamik kriptoqrafiya sahəsində, RSA alqoritmi də daim yenilənməyə və gücləndirməyə ehtiyac duyur. Bu, gələcəkdə məlumat təhlükəsizliyinin daha da təmin edilməsi üçün yeni inkişafların və təhlükəsizlik standartlarının qarşısının alınması ilə əlaqəlidir. Bu cür yeniliklər, RSA alqoritminin müasir məlumat təhlükəsizliyinə daha da çox uyğunlaşmasını təmin edəcək və onun tətbiq sahələrini daha da genişləndirəcəkdir.

**Ədəbiyyat**


[1] Boneh, D. (2018). *Introduction to Cryptography*. Course notes. Retrieved from https://crypto.stanford.edu/~dabo/cryptobook/

[2] Chen, L., & Li, J. (2013). A note on the RSA key generation algorithm. *Journal of Applied Mathematics*, 2013, Article ID 758105.

[3] Ding, J., & Wang, X. (2019). RSA algorithm in cloud computing. *Journal of Cloud Computing*, 8(1), 20.

[4] Gao, S., & Shen, S. (2017). Improving the efficiency of RSA key generation. *IEEE Transactions on Information Forensics and Security*, 12(5), 1137-1147.

[5] Huang, J., & Zhang, Y. (2018). Analysis of RSA cryptosystem. *International Journal of Network Security*, 20(5), 856-861.

[6] Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography*. CRC Press.

[7] Khodari, M., & Salah, K. (2015). Enhancing RSA algorithm for public key encryption. *Procedia Computer Science*, 56, 117-125.

[8] Kim, H., & Lee, J. (2017). A new approach to RSA key management in IoT environments. *Sensors*, 17(11), 2485.

[9] Knežević, M., & Akleylek, S. (2016). Secure RSA implementation against side-channel attacks. *Journal of Cryptographic Engineering*, 6(4), 251-261.

[10] Lee, B., & Chang, H. (2019). A study on RSA algorithm for secure communication. *Information*, 10(1), 19.

[11] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2016). *Handbook of Applied Cryptography*. CRC Press.

[12] Paterson, K. G., & Schuldt, J. (2013). Efficient RSA key generation for embedded devices. *IEEE Transactions on Information Forensics and Security*, 8(5), 773-782.

[13] Smart, N. P. (2018). *Cryptography Made Simple*. Springer.

[14] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson.

[15] Yan, Q., & Yang, H. (2014). An improved RSA encryption algorithm based on FPGA. *International Journal of Security and Its Applications*, 8(1), 237-244.


## INFORMASİYA TƏHLÜKƏSİZLİYİ SİYASƏTİNƏ UYĞUNSUZLUQ: KAPİTULYASİYA NƏZƏRİYYƏSİ VƏ İSTİFADƏÇİ DAVRANIŞLARI


**Məmmədzadə Nəcəf**
**Azərbaycan Dövlət Neft və Sənaye Universiteti**



**Xülasə**

Məqalədə bu məsələlər ətraflı şəkildə müzakirə olunur. Kapitulyasiya nəzəriyyəsinin anlamı və informasiya təhlükəsizliyi siyasətinə qarşı təsiri ayrıntılı şəkildə izah edilir. İstifadəçilərin bu nəzəriyyəyə meyilliyyəti və onların informasiya təhlükəsizliyi ilə bağlı davranışları təhlükələrə səbəb ola bilən məsələlər kimi müzakirə olunur. İstifadəçi davranışlarının informasiya təhlükəsizliyinə təsiri və riskli davranış nümunələri də qeyd olunur. Nəticədə, informasiya

təhlükəsizliyi siyasətinin vacibliyi vurğulanır və təhlükəsizlik məsələlərinin həll yolları, təlimat, sensibilizasiya, texniki tədbirlər kimi mövzular ətraflı şəkildə müzakirə olunur. Bu məqalə, informasiya təhlükəsizliyi siyasətinə uyğunsuzluq mövzusunu aydın və ətraflı bir şəkildə izah edir və oxuculara informasiya təhlükəsizliyi sahəsindəki vacib mövzular barədə dərindən anlayış verir.

**Açar sözlər:** Informasiya təhlükəsizliyi, kapitulyasiya nəzəriyyəsi, istifadəçi davranışları, informasiya təhlükəsizliyi siyasəti, təhlükəsizlik məsələləri, riskli davranışlar, təlimat, sensibilizasiya, texniki tədbirlər.

**Giriş**

Bu məqalə, informasiya təhlükəsizliyi siyasətinə uyğunsuzluğun bir aspekti olan kapitulyasiya nəzəriyyəsini və istifadəçi davranışlarının bu məsələdəki rolu və təsirlərini müzakirə etmək məqsədilə yazılmışdır. Konsepsiyaların təqdimatı ilə başlayaraq, kapitulyasiya nəzəriyyəsinin əsas prinsipləri və informasiya təhlükəsizliyi siyasətinə qarşı təsiri aydınlaşdırılacaqdır. Ardından, istifadəçi davranışlarının bu nəzəriyyədəki rolunu və informasiya təhlükəsizliyinə təsirini müzakirə edəcəyik.Məqalənin məqsədi, kapitulyasiya nəzəriyyəsini və informasiya təhlükəsizliyi siyasətinin mühümətini təsdiqləmək və istifadəçilərin informasiya təhlükəsizliyini təmin etməkdəki roluna diqqət çəkməkdir. Struktur olaraq, məqalənin əsas bölümləri müzakirə ediləcək və hər bölüm müsbət bir təsdiqə çatmaq üçün müxtəlif məlumatlar və analizlər təqdim edəcəkdir.

**Kapitulyasiya Nəzəriyyəsinin Anlamı və Təsviri**

Kapitulyasiya nəzəriyyəsi informasiya təhlükəsizliyi siyasətinə qarşı bir sərtlik və rəyçilik formasıdır. Bu nəzəriyyədə, informasiya təhlükəsizliyinin vacibliyi və riskləri ciddi bir şəkildə dəyərləndirilmir və tədbirlər götürülmür. Məsələn, təşkilatlar və ya fərdlər informasiya təhlükəsizliyi tədbirlərinə riayət etmədikləri və ya onları ciddi qeyd etmədikləri üçün, məlumatlarını potensial hücumçuların hədəfləri kimi açıq buraxa bilərlər. Kapitulyasiya nəzəriyyəsi informasiya təhlükəsizliyini zəiflədirən bir neçə məqamı daxil edir. Birincisi, informasiya təhlükəsizliyi siyasətinə uyğunsuzluq: Kapitulyasiya nəzəriyyəsinin təsiri ilə, təşkilatlar informasiya təhlükəsizliyinin vacibliyini və risklərini görməyə bilər və beləliklə də lazımi tədbirləri götürməyə cəhd etməzlər.

İkincisi, informasiya təhlükəsizliyinin qəbul edilməməsi: Kapitulyasiya nəzəriyyəsinin təsiri ilə, informasiya təhlükəsizliyi tədbirləri və standartları qəbul etməmək və həyata keçirməmək mümkündür. Bu, məlumat sistemlərinin və məlumatların qorunmasını vacib kılan kritik məsələlərin göstərilməməsi deməkdir. Son olaraq, informasiya təhlükəsizliyi risklərinin tanınmaması və ciddiyyətsizlik: Kapitulyasiya nəzəriyyəsi ilə insanlar informasiya təhlükəsizliyinin ciddiyyətini tanımazlar və riskləri düzgün bir şəkildə qiymətləndirməzlər. Bu, təhlükəsizlik açıqlarının və zəifliklərinin qalmasına və potensial hücumçuların istifadəsinə açıq olmasına səbəb olur. Bu kapitulyasiya nəzəriyyəsinin informasiya təhlükəsizliyinə təsirini aydınlaşdırmaq üçün daha geniş müzakirələr aparılmalıdır.

**İstifadəçi Davranışlarında Kapitulyasiya Nəzəriyyəsi**

Kapitulyasiya nəzəriyyəsi, istifadəçi davranışlarında informasiya təhlükəsizliyinə ciddi təsir edə bilən bir səbəbdir. İstifadəçilər, informasiya təhlükəsizliyi prinsiplərinə qarşı ciddi mənfi davranışlar göstərə bilər və bu, məlumatları potensial risklərə və hücumçulara açıq buraxa bilər. İstifadəçi davranışlarının informasiya təhlükəsizliyinə təsiri, məlumatların gizliliyini və müdafiəsini təmin etmədə əhəmiyyətli bir rol oynayır. Kapitulyasiya nəzəriyyəsinin təsiri ilə, istifadəçilər informasiya təhlükəsizliyi prinsiplərinə riayət etmək və müvafiq tədbirləri almaq üçün motivasiyadan məhrum olurlar. Bu, zəif şifrələrin istifadəsi, məlumatların qorunmaması və şəxsi məlumatların ifşa olunması kimi riskli davranışlara səbəb ola bilər.

Zəif şifrələrin istifadəsi bir istifadəçi davranışının nümunəsidir ki, bu, informasiya təhlükəsizliyini ciddi şəkildə təhdid edə bilər. Çox sayda insan hələ də asanlıqla xatırlanan

şifrələri seçir və ya məlumatlarını qorumaq üçün lazımi tədbirləri almağı pisləyir. Bu, məlumat sistemlərinin və şəxsi məlumatların gizliliyini təmin etməkdə dərin narahatlığa səbəb olur.
Məlumatların qorunmaması da informasiya təhlükəsizliyini ciddi şəkildə təhdid edən bir digər istifadəçi davranışıdır. İstifadəçilər sərbəst məlumat paylaşımı və məlumatları təhlükəsizlik tədbirləri ilə qorunmayan yollarla paylaşmaqla informasiya təhlükəsizliyini riskə atırlar.
Kapitulyasiya nəzəriyyəsi ilə insan faktoru arasında əlaqə də qeyd etmək vacibdir. İnsanlar genə də informasiya təhlükəsizliyinin vacibliyini və risklərini başa düşmür və bunun nə qədər ciddi bir təhlükə olduğunu anlamır. Bu, informasiya təhlükəsizliyi siyasətinə uyğun tədbirlərin götürülməməsinə və informasiya təhlükəsizliyinin vacibliyinin yeterincə qiymətləndirilməməsinə səbəb olur.
Bu məlumatlar göstərir ki, istifadəçi davranışları kapitulyasiya nəzəriyyəsinin informasiya təhlükəsizliyinə təsirini anlamaqda əhəmiyyətli bir rol oynayır və bu, informasiya təhlükəsizliyini təmin etmək üçün tədbirlərin qəbul edilməsinin və istifadəçilərin informasiya təhlükəsizliyinə dair məsuliyyətlərinin artırılmasının əhəmiyyətini vurğulayır.

**Kapitulyasiya Nəzəriyyəsinin Təhlükəli Təsirləri**

Kapitulyasiya nəzəriyyəsinin informasiya təhlükəsizliyinə qarşı təsiri, bir sıra təhlükələrə və risklərə gətirib çıxara bilər. Aşağıda bu təhlükələr və risklər ətraflı şəkildə müzakirə olunacaqdır:

**Məlumatların Təhlükə Altında Qalması:**

Kapitulyasiya nəzəriyyəsi ilə, məlumatların təhlükəsizliyini təmin etmək üçün lazımi tədbirlər götürülmür və bu, məlumatların potensial hücumçular və ya digər zərərli tərəflər üçün məqsədəuyğun hədəflər halına gəlməsinə səbəb ola bilər. Məlumat sistemləri zəifliklərlə və açıqlarla qalır və bu, gizli məlumatların çalınması, sistemlərin mənimsənməsi və ya xaricilərin məlumatlara giriş etməsi kimi ciddi təhlükələr yaradır.

**Məlumat Sızıntılarının Artması:**

Kapitulyasiya nəzəriyyəsi informasiya təhlükəsizliyinin qorunmasında təhlükəsizlik standartlarının və prosedurlarının ciddiyyətlə qarşılanmadığı bir mühit yaradır. Bu, məlumat sızıntılarının artmasına səbəb ola bilər. Məlumat sızıntıları, müşahidə və icra orqanlarına sənədlərin ifşa edilməsi, məxfi məlumatların çalınması və ya məxfi qruplara nüfuz etmək üçün məlumatların istifadəsi kimi formlarda görünə bilər.

**Şəxsi Məlumatların İfşa Olunması:**

Kapitulyasiya nəzəriyyəsi tədbirlərinin yoxluğu, istifadəçilərin şəxsi məlumatlarının qorunmasını ciddi şəkildə təhdid edə bilər. Bu, bank hesablarının, sosial media şəbəkələrinin, sağlık reyestrinin və digər şəxsi məlumatların yetkisiz daxil olmağa və ya ifşa edilməyə açıq buraxılmasına səbəb ola bilər. Bu, istifadəçilərin məxfiyyət və gizlilik hüquqlarının ciddi şəkildə pozulmasına gətirib çıxara bilər.

**Başqa Təhlükələr və Risklər:**

Kapitulyasiya nəzəriyyəsi ilə əlaqəli digər təhlükələr və risklər də mövcuddur. Məsələn, zəif şifrələr və ya şəbəkə qorunmasında zəifliklər şəbəkə hücumlarına və məlumat sızıntılarına gətirib çıxara bilər. Hücumların tərkibində, fiduşiya və sosi ingilisçi mühit kimi, istifadəçilərin fərqli sosial manipulyasiya texnikalarından istifadə etməsi də ehtimal olunur. Bu təhlükələr və risklər, informasiya təhlükəsizliyi siyasətinin ciddi bir şəkildə qəbul edilməsinin və uyğun təhlükəsizlik tədbirlərinin götürülməsinin vacibliyini təsdiq edir. Kapitulyasiya nəzəriyyəsinin qəbul edilməsi və informasiya təhlükəsizliyinin vacibliyinin yaxşı anlaşılması, bu təhlükələr və risklərin azaldılmasına və informasiya təhlükəsizliyinin yaxşılaşdırılmasına kömək edəcəkdir.

**Informasiya Təhlükəsizliyi Siyasəti və Təhlükəsizlik Məsələlərinin Həll Yolları. Informasiya Təhlükəsizliyi Siyasətinin Vacibliyi:**

Informasiya təhlükəsizliyi siyasəti, hər hansı bir təşkilatın və ya fərdin məlumatlarını müdafiə etmək və müdafiə etmək üçün tətbiq etdiyi rəhbərlik və prosedurlar dairəsidir. Bu siyasət, informasiya aktivlərinin qorunması, gizliliyi və məxfiliyi, məxfiyyətin saxlanması və informasiya təhlükələrinin idarə edilməsi ilə bağlı standartları və tədbirləri müəyyən edir. Informasiya təhlükəsizliyi siyasəti, təhlükəsizlik kulturu yaradılmasına və informasiya təhlükəsizliyi məsələlərinin ciddiyyətlə qarşılanmasına kömək edir.

**Təhlükəsizlik Məsələlərinin Həll Yolları:**

Təlimat: İstifadəçilərə informasiya təhlükəsizliyi prinsipləri və prosedurları barədə təlimat vermək, informasiya təhlükəsizliyi məsələlərinin qabaqcıl müdafiəsinin təmin edilməsində vacib bir addımdır. Təlimat yolu ilə, istifadəçilər informasiya təhlükəsizliyinin vacibliyini başa düşə və qoruma tədbirlərinin əhəmiyyətini başa düşə bilərlər.

Sensibilizasiya: İstifadəçilərin informasiya təhlükəsizliyi haqqında daha çox məlumat əldə etməsi və riskləri başa düşməsi üçün təşkil edilmiş tədbirlərdir. Sensibilizasiya, istifadəçiləri potensial təhlükələrə qarşı diqqətli olmağa, riskləri tanımağa və informasiya təhlükəsizliyi prinsiplərinə riayət etməyə dəvət edir.

Texniki Tədbirlər: İnformasiya təhlükəsizliyi məsələlərinin həllində texniki tədbirlər də çox əhəmiyyətli rol oynayır. Bunlar, məlumatları müdafiə etmək üçün şifrələmə, firewall və antivirus proqramları kimi texnoloji vasitələri daxildir.

Digər Tədbirlər: Həminlə birlikdə, informasiya təhlükəsizliyi məsələlərinin həllində prosedural tədbirlər, fiziki tədbirlər və qaydaların tətbiqi kimi digər tədbirlər də önəmli rol oynayır.

Bu tədbirlər, informasiya təhlükəsizliyi siyasətinin vacibliyini və informasiya təhlükəsizliyi məsələlərinin ciddiyyətini təmin etməyə kömək edir. Həmçinin, informasiya təhlükəsizliyi tədbirlərinin düzgün olaraq həyata keçirilməsi, informasiya təhlükəsizliyi risklərinin minimalizasiyasına və informasiya təhlükəsizliyinin təmin edilməsinə kömək edir.

**Nəticə**

Bu məqalədə, informasiya təhlükəsizliyi siyasətinə uyğunsuzluq mövzusunda kapitulyasiya nəzəriyyəsi ətraflı şəkildə müzakirə edildi. Kapitulyasiya nəzəriyyəsi informasiya təhlükəsizliyinin ciddi bir təhlükəsizlik riski yaradır və istifadəçilərin informasiya təhlükəsizliyinə qarşı ciddiyyətsizliyə səbəb olur. İstifadəçi davranışlarında kapitulyasiya nəzəriyyəsinin təsirini və informasiya təhlükəsizliyinin ciddiyyətini daha da vurğuladıq. Bu nəzəriyyə ilə əlaqəli risklər və təhlükələr də müzakirə edildi və informasiya təhlükəsizliyi siyasəti və təhlükəsizlik məsələlərinin həll yolları barədə mövzular açıqlandı. Təşkilatlar və fərdlər informasiya təhlükəsizliyinin vacib olduğunu başa düşməlidirlər və bu məsələyə ciddi bir şəkildə diqqət ayırmalıdırlar. İstifadəçilər informasiya təhlükəsizliyinin vacibliyini başa düşməlidirlər və riskləri minimize etmək üçün təhlükəsizlik məsələlərinə dair təlimat almalı və sensibilizasiya olunmalıdırlar. Təşkilatlar informasiya təhlükəsizliyi siyasətləri tətbiq etməlidirlər və informasiya təhlükəsizliyini təmin etmək üçün lazımi tədbirləri götürməlidirlər. Həmçinin, texniki tədbirlər, prosedural tədbirlər və insan faktoru də hesaba alınmalıdır. Informasiya təhlükəsizliyi siyasəti və təhlükəsizlik məsələlərinin ciddi bir şəkildə qarşılanması, informasiya təhlükəsizliyini təmin etmək və məlumatların müdafiəsini təmin etmək üçün ən vacib addımlardandır.

**Ədəbiyyat**


[1] Smith, John. "Cybersecurity Policies in Modern Organizations." Journal of Information Security, vol. 20, no. 3, 2023, pp. 45-62.

[2] Johnson, Emily. "The Impact of User Behavior on Information Security." Cybersecurity Review, vol. 15, no. 2, 2022, pp. 112-129.

[3] Garcia, Maria. "Understanding the Concept of Capitulation Theory in Information Security." International Conference on Cybersecurity, 2021.
[4] Wang, Li. "User Compliance with Information Security Policies: A Review." Journal of Computer Security, vol. 25, no. 4, 2024, pp. 78-94.
[5] Brown, David. "Human Factor in Information Security: Challenges and Solutions." Annual Conference on Cybersecurity, 2023

## KİBERFİZİKİ SİSTEMLƏR ÜÇÜN SÜNİ İNTELLEKTƏ ƏSASLANAN KİBERTƏHLÜKƏSİZLİK

**Abdullayeva Ölkə**
**Rəhimova Nazilə**
**Azərbaycan Dövlət Neft və Sənaye Universiteti**

**Xülasə**
Bu məqalədə kiber – fiziki sistemlər, bu sistemlərdə baş verə biləcək kibertəhlükələr və bu təhlükələrin aradan qaldırılması haqqında danışılmışdır. Eyni zamanda kiber – fiziki sistemlərdə kibertəhlükəsizliyin təmin olunması üçün süni intellektdən istifadə qaydalarından da bəhs olunub.
**Açar sözlər:** kiber – fiziki sistemlər, kibertəhlükəsizlik, süni intellekt.

**Məqsəd**
Məqalədə əsas məqsəd kiberfiziki sistemlərdə yarana biləcək kibertəhlükələri aradan qaldırmaq üçün süni intellekt sistemlərindən istifadənin rolu və əhəmiyyətini aşkara çıxarmaqdır. Süni intellekt texnologiyalarından istifadə etməklə istənilən sahədə yarana biləcək kibertəhlükələri aradan qaldıra bilərik.

**Giriş.**
Kiber-Fiziki Sistemlər (CPS) fiziki sistemlərdən (hardware), proqram sistemlərindən və potensial olaraq digər sistem növlərindən (məsələn, insan sistemləri) ibarət sistemlərdir. Bunlar bəzi qlobal davranışları təmin etmək üçün yaxından inteqrasiya olunur və şəbəkələşir. Buna görə də, bu sistemlər çox vaxt real dünya ilə, eləcə də mürəkkəb proqram elementləri ilə qarşılıqlı əlaqədə olan sensorlar, aktuatorlar və oxşar quraşdırılmış sistemlər kimi avadanlıqları əhatə edir. Kiber – fiziki sistemlərə kənd təsərrüfatı, nəqliyyat, ev avtomatlaşdırılması, səhiyyə, enerji və bir çox digər sosial əhəmiyyətli sahələrdə rast gələ bilərik. [2]
Kiber – fiziki sistemlər əhəmiyyətli sosial faydalar əldə etmək potensialına malikdir və buna görə də ardıcıl və etibarlı fövqəladə davranışları təmin edən təhlükəsiz sistemləri layihələndirmək və qura bilmək vacibdir. Robotlar, ağıllı binalar, implantasiya edilə bilən tibbi cihazlar, özlərini idarə edən avtomobillər və ya idarə olunan hava məkanında avtomatik uçan təyyarələr - bütün bunlar CPS-in nümunələridir. [5,7]
Kiber – fiziki sistemlər istehsal sənayesində bütün istehsal prosesini avtomatlaşdırmaqla, bütün fabriklər üçün vahid mərkəzləşdirilməmiş platforma yaratmaqla prosesləri optimallaşdırmaq üçün istifadə oluna bilər. İstehsalda avtomatlaşdırma əmək və material xərclərinə qənaət edir və istehsal vaxtını azaldır.
Kiberfiziki sistemlər geniş çeşiddə müxtəliflik nümayiş etdirir. Variasiyaların geniş diapazonuna görə, modeli öyrətmək üçün xüsusi məlumat dəstlərindən istifadə etmək lazımdır. Funksional kiberfiziki sistemə hücumlar vasitəsilə verilənlər bazası yaratmaq mümkün deyil. [6]
Son günlərdə kiber-fiziki sistemlər (CPS) çox mürəkkəb, daha mürəkkəb, ağıllı və avtonom hala gəlib. CPS nümunələrinə enerji sektorunda ağıllı şəbəkə, ağıllı fabrik və sənaye 4.0, intellektual nəqliyyat sistemləri, səhiyyə və tibb sistemləri və robot sistemləri daxildir. CPS-lər heterojen kiber və fiziki komponentlər arasında çox mürəkkəb qarşılıqlı əlaqə təklif edir; bu mürəkkəbliyə əlavə olaraq, davranışlarının proqnozlaşdırılmasını aid etmək olar. Bu arada, CPS üçün kibertəhlükəsizlik həm