ISSN: 1609-1620
VOLUME 27 ISSUE 06 2025
PAHTEI
REFEREED & REVIEWED JOURNAL
Pp. 37-44 DOI: https://doi.org/10.32010/AKNM5375

ANALYSIS OF REMOTE ATTACKS AND CURRENT DEFENSE SYSTEMS

Vagif Karimov[1], Jabbar Hasanov[2]
[1,2]Azerbaijan State Oil and Industry University
[1]Department of General and Applied Mathematics
[2]Department of Computer engineering
[1]Docent, Candidate of technical sciences, kvaqif56@gmail.com
[2]Master student, cabbarhesenov1999@gmail.com

ABSTRACT

Remote attacks are one of the most serious threats to cybersecurity in the field of information technologies. These attacks are carried out without direct physical contact, via the Internet or other network channels. Remote attacks include a wide range of attack methods such as DDoS (Distributed Denial of Service), remote distribution of malware, phishing, SQL injection, remote code execution and man-in-the-middle (MITM). These attacks can lead to infrastructure paralysis, theft of confidential information and economic losses. Among the existing defense systems, firewalls, antivirus software, network traffic analysis systems (IDS/IPS), encryption protocols (TLS, VPN), multi-factor authentication and artificial intelligence-based threat detection systems play an important role. Against the backdrop of the increase in remote attacks, it has become necessary to continuously update cybersecurity strategies. Due to the flexibility and sophistication of attack vectors, traditional defense mechanisms alone are not enough. For this reason, proactive security approaches, i.e. methods for identifying and mitigating risks before an attack, are coming to the fore. Using scanners to automatically detect security vulnerabilities, regularly updating systems (patching) and conducting security tests are important technical measures. In addition, forming a security culture in enterprises and regularly involving staff in training also play a decisive role in reducing risks related to the human factor. Since phishing and social engineering attacks mainly exploit human weaknesses, awareness-raising measures in this area are as important as technical measures. Among the innovative approaches, artificial intelligence (AI) and machine learning (ML)-based systems stand out in particular. These technologies can analyze large volumes of network data and distinguish between normal and abnormal behavior, thus allowing for the detection of attacks at an early stage. For example, SIEM (Security Information and Event Management) and UEBA (User and Entity Behavior Analytics) systems, which identify unusual activity of user accounts based on behavioral analysis, have become an integral part of modern cybersecurity architecture. At the same time, the Zero Trust model is also widely used in modern security strategies. According to this model, no user or device is trusted in advance, and the principle of re-verification of any access is applied. Thus, attacks carried out from the internal network are prevented more effectively. Regulatory legal frameworks and standards adopted at the state and international levels also play an important role in the development of this area. For example, data protection legislation such as GDPR (General Data Protection Regulation of the European Union) obliges organizations to take more serious security measures. Such rules serve to ensure the security of the cyber environment by defining not only technical, but also ethical and legal frameworks.

Keywords: remote attacks, cybersecurity, defense systems, remote code execution, intrusion detection systems (IDS/IPS)

MƏSAFƏDƏN HÜCUMLARIN TƏHLİLİ VƏ MÖVCUD MÜDAFİƏ SİSTEMLƏRİ

Vaqif Kərimov[1], Cabbar Həsənov[2]

PAHTEI
REFEREED & REVIEWED JOURNAL
ISSN: 1609-1620
VOLUME 27 ISSUE 06 2025

[1,2]Azərbaycan Dövlət Neft və Sənaye Universiteti
[1]"Ümumi və tətbiqi riyaziyyat" kafedrası
[2]"Kompüter mühəndisliyi" kafedrası
[1]Dosent, texnika elmləri namizədi, kvaqif56@gmail.com
[2]Magistr tələbəsi, cabbarhesenov1999@gmail.com

XÜLASƏ

Məsafədən hücumlar (remote attacks) informasiya texnologiyaları sahəsində kibertəhlükəsizlik üçün ən ciddi təhdidlərdən biridir. Bu hücumlar birbaşa fiziki əlaqə olmadan, internet və ya digər şəbəkə kanalları vasitəsilə həyata keçirilir. Məsafədən hücumlara DDoS (Distributed Denial of Service), zərərverici proqramların (malware) uzaqdan yayılması, phishing, SQL injection, remote code execution və man-in-the-middle (MITM) kimi geniş spektrli hücum metodları daxildir. Bu hücumlar infrastrukturun iflicinə, məxfi məlumatların oğurlanmasına və iqtisadi zərərlərə səbəb ola bilər. Bundan əlavə, müəssisələrdə təhlükəsizlik mədəniyyətinin formalaşdırılması və işçi heyətinin mütəmadi şəkildə təlimə cəlb olunması da insan faktoru ilə əlaqəli risklərin azaldılmasında həlledici rol oynayır. Phishing və sosial mühəndislik (social engineering) hücumları əsasən insan zəifliyindən istifadə etdiyi üçün bu sahədəki maarifləndirmə tədbirləri texniki tədbirlər qədər əhəmiyyətlidir. İnnovativ yanaşmalar sırasında süni intellekt (AI) və maşın öyrənməsi (ML) əsaslı sistemlər xüsusilə fərqlənir. Beləliklə, daxili şəbəkədən həyata keçirilən hücumların qarşısı daha effektiv şəkildə alınır. Dövlət və beynəlxalq səviyyədə qəbul edilən normativ hüquqi bazalar və standartlar da bu sahənin inkişafında əhəmiyyətli rol oynayır. Məsələn, GDPR (Avropa İttifaqının Ümumi Məlumatların Qorunması Qaydaları) kimi məlumatların qorunması qanunvericiliyi təşkilatları daha ciddi təhlükəsizlik tədbirləri görməyə məcbur edir. Bu tip qaydalar yalnız texniki deyil, həm də etik və hüquqi çərçivəni müəyyənləşdirərək kibermühitin təhlükəsizliyini təmin etməyə xidmət edir.

Açar sözlər: məsafədən hücumlar, kibertəhlükəsizlik, müdafiə sistemləri, uzaqdan kod icrası (Remote Code Execution), təhlükə aşkarlama sistemləri (IDS/IPS

Giriş

Məsafədən hücumların genişlənməsi yalnız texniki məsələlərlə məhdudlaşmır, eyni zamanda sosial mühəndislik üsulları ilə də sıx bağlıdır. Hücum edənlər istifadəçilərin psixoloji zəif cəhətlərindən, diqqətsizliklərindən və məlumatlılıq səviyyəsinin aşağı olmasından istifadə edərək sistemlərə daxil olurlar. Bu da göstərir ki, təhlükəsizlik yalnız proqram təminatı və avadanlıqlarla deyil, həm də insan faktorunun nəzərə alınması ilə təmin olunmalıdır.

Bundan əlavə, qlobal miqyasda baş verən kibertəhdidlərin transsərhəd xarakter daşıması beynəlxalq əməkdaşlığın və standartlaşdırılmış müdafiə sistemlərinin vacibliyini gündəmə gətirir. Bir çox ölkələr artıq informasiya təhlükəsizliyi üzrə milli strategiyalar hazırlayır, kritik infrastrukturlar üçün xüsusi müdafiə protokolları tətbiq edirlər. Azərbaycan da bu sahədə irəliləyişlərə nail olmaq üçün hüquqi baza və texnoloji sistemlərini təkmilləşdirmək istiqamətində mühüm addımlar atır.

Mövzuya dair aparılan bu tədqiqatın əsas məqsədi məsafədən hücumların mahiyyətini dərin şəkildə təhlil etmək, onların texniki və sosial aspektlərini araşdırmaq və mövcud müdafiə sistemlərinin effektivliyini qiymətləndirməklə yanaşı, gələcəkdə daha dayanıqlı və çevik təhlükəsizlik mexanizmlərinin yaradılmasına töhfə verməkdir. Eyni zamanda, süni intellekt və maşın öyrənməsi texnologiyalarının bu sahəyə inteqrasiyasının perspektivləri də araşdırılacaq. Bu yanaşma, informasiya təhlükəsizliyinin proaktiv və adaptiv metodlarla təmin olunmasının vacibliyini bir daha ön plana çıxarır.

Rəqəmsallaşma prosesinin sürətlənməsi və qlobal şəbəkələrin genişlənməsi ilə yanaşı, informasiya sistemlərinə qarşı həyata keçirilən məsafədən hücumların miqyası və intensivliyi də əhəmiyyətli dərəcədə artmışdır. Bu cür hücumlar texnoloji infrastrukturun zəif nöqtələrindən istifadə edərək, sistemlərə uzaq məsafədən zərər yetirməyə və ya məxfi məlumatları ələ keçirməyə imkan verir. Xüsusilə dövlət qurumları, bank sektoru, enerji infrastrukturları və şəxsi məlumat bazaları məsafədən hücumlar üçün əsas hədəflər sırasındadır. Hücumların müxtəlifliyi – DDoS hücumları, zərərverici

proqramların yayılması, şəbəkə üzərindən idarə olunan hücumlar və istifadəçi identifikasiyasının oğurlanması – informasiya təhlükəsizliyinin daha mürəkkəb və çoxtərəfli müdafiə tədbirləri ilə təmin olunmasını zəruri edir.

Mövcud müdafiə sistemlərinin tətbiqi və inkişafı bu sahədə baş verən sürətli texnoloji dəyişikliklərə adekvat şəkildə cavab verməlidir. Klassik firewall-lardan tutmuş, süni intellektlə dəstəklənən təhdid aşkarlama sistemlərinə qədər müxtəlif müdafiə mexanizmləri bu məqsədə xidmət edir. Bu tədqiqatda məsafədən hücumların növləri, onların əsas xüsusiyyətləri və yaratdığı təhlükələr təhlil olunacaq, mövcud müdafiə sistemlərinin effektivliyi dəyərləndiriləcək və gələcəkdə tətbiq edilə biləcək texnoloji yanaşmalara nəzər salınacaq. Mövzunun aktuallığı ondan ibarətdir ki, informasiya təhlükəsizliyi sahəsində baş verən yeniliklər və təhdidlərin çevik şəkildə təhlili həm fərdi istifadəçilərin, həm də təşkilatların davamlı fəaliyyətini və məlumat təhlükəsizliyini təmin etmək baxımından həyati əhəmiyyət daşıyır.

Müasir dövrdə informasiya texnologiyalarının həyatın bütün sahələrinə nüfuz etməsi ilə təhlükəsizlik məsələləri daha da aktuallaşmışdır. Xüsusilə məsafədən idarə olunan hücumlar istər dövlət qurumları, istərsə də özəl sektor üçün ciddi təhlükə mənbəyinə çevrilmişdir. Bu hücumlar yalnız texnoloji zərərlə kifayətlənmir, eyni zamanda iqtisadi itkilər, sosial çaxnaşmalar və reputasiya riskləri yarada bilər. Buna görə də məsafədən hücumların qarşısının alınması və onların yaratdığı təhdidlərin idarə olunması təkcə informasiya texnologiyaları mütəxəssislərinin deyil, həm də qərarverici orqanların və strateji səviyyədə idarəetmə strukturunun əsas prioritetlərindən biri olmalıdır.

Hazırkı dövrdə informasiya sistemlərinə edilən məsafəli hücumların təhlili göstərir ki, ənənəvi müdafiə metodları bəzən kifayət etmir. Hücumların daha mürəkkəb və kamuflyajlı şəkildə həyata keçirilməsi, zərərverici kodların adaptiv xarakter daşıması və sıfır-gün (zero-day) zəifliklərə yönəlməsi yeni texnoloji yanaşmaların və qabaqlayıcı müdafiə sistemlərinin vacibliyini artırır. Burada süni intellekt və böyük verilənlərin analizi kimi qabaqcıl texnologiyaların tətbiqi daha çevik və proqnozlaşdırıcı təhlükəsizlik siyasətlərinin qurulmasında əsas rol oynaya bilər.

Eyni zamanda, məsafədən hücumların qarşısının alınmasında istifadəçi davranışlarının və təşkilati mədəniyyətin də mühüm təsiri vardır. İnformasiya təhlükəsizliyinin yalnız texnoloji vasitələrlə deyil, həm də təşkilati və hüquqi müstəvidə kompleks şəkildə qurulması bu tədqiqatın əsas tezislərindən birini təşkil edir. Nəticə etibarilə, məsafədən hücumların effektli şəkildə qarşısının alınması üçün texnoloji innovasiyalar, normativ hüquqi çərçivə və insan amili arasında balanslaşdırılmış yanaşma zəruridir. Bu baxımdan tədqiqatda təqdim ediləcək təhlil və nəticələr informasiya təhlükəsizliyi sahəsində daha dayanıqlı və inteqrasiyalı strategiyaların formalaşdırılmasına xidmət edir.

Ədəbiyyat icmali. Məsafədən hücumlar və bu hücumlara qarşı mövcud müdafiə sistemləri son illərdə kibertəhlükəsizlik sahəsində aparılan tədqiqatların əsas istiqamətlərindən birini təşkil edir. Ədəbiyyatın təhlili göstərir ki, məsafədən həyata keçirilən kibertəhdidlər yalnız texniki zəifliklərdən deyil, həm də təşkilati boşluqlardan qaynaqlanır. Kruse və digər tədqiqatçılar (2017) səhiyyə sahəsində məsafədən hücumların təhlükəli nəticələrini vurğulayaraq göstərirlər ki, sistemlərdəki zəif autentifikasiya və şifrələmə mexanizmləri məlumatların sızmasına səbəb olur. Eyni zamanda Romanosky və digərlərinin (2019) apardığı araşdırmalar göstərir ki, kibersığorta siyasətləri bu risklərin idarə olunmasında hələ də yetərli deyil, çünki risk qiymətləndirməsi standartlaşdırılmamışdır.

Loukas və həmkarları (2013) tərəfindən aparılmış araşdırmada məsafədən hücumlar fərqli təsnifatlara bölünərək təhlil olunur və göstərilir ki, real zamanlı təhdid aşkarlama sistemləri (IDS/IPS) bu cür hücumların qarşısını almaqda əsas vasitələrdən biridir. Eyni zamanda, Eling və Schnell (2016) məsafədən hücumların maliyyə sektoru üçün yaratdığı itkilərin təhlilinə yönəlmiş tədqiqatlarında qeyd edirlər ki, bu hücumların nəticələri yalnız texnoloji deyil, həm də iqtisadi baxımdan böyük ziyanlara səbəb olur.

Mövzunun digər aspektinə toxunan Maleks Smith və digərləri (2022) qeyd edirlər ki, mövcud statistik bazaların və təhlükə məlumatlarının məhdudluğu məsafədən hücumlara qarşı effektiv risk modellərinin qurulmasını çətinləşdirir. Bu isə, öz növbəsində, qərarverici qurumların və təşkilatların proqnozlaşdırıcı müdafiə tədbirləri görməsinə mane olur. Bununla yanaşı, Zhou və Leung (2023) məsafədən hücumların yeni trendlərini və süni intellektin müdafiə sistemlərində tətbiqini araşdıraraq göstərirlər

ki, maşın öyrənməsi və böyük verilənlərin təhlili kibertəhlükələrin aşkarlanması və cavab müddətinin optimallaşdırılmasında perspektivli vasitədir.

Ədəbiyyat icmalının davamı olaraq qeyd etmək lazımdır ki, məsafədən hücumların spesifikliyi onların çox zaman aşkarlanmasının çətin və gecikmiş olması ilə xarakterizə olunur. Bu xüsusiyyət tədqiqatlarda geniş şəkildə vurğulanır. Məsələn, Ulven və Wangen (2021) ali təhsil müəssisələrində kibertəhlükəsizlik risklərinin sistemli təhlilini apararaq göstərirlər ki, insan amili və məlumat axınlarının zəif nəzarəti məsafədən həyata keçirilən hücumların qarşısının alınmasında əsas maneələrdəndir. Bu kontekstdə insan davranışlarının modelləşdirilməsi və təhlükəsizlik mədəniyyətinin təşviqi müasir müdafiə siyasətlərinin mühüm komponenti kimi qiymətləndirilir.

Eyni zamanda "Lee and Lee" (2020) İnternet əşyaları (IoT) ilə bağlı tətbiqləri və bu sistemlərin məsafədən hücuma qarşı həssaslığını araşdıraraq bildirirlər ki, bu cür texnologiyaların genişlənməsi təhlükəsizlik tədbirlərinin yenidən düşünülməsini və daha çevik həllərin tətbiqini tələb edir. İoT cihazlarının zəif təhlükəsizlik mexanizmləri və proqram təminatı yeniləmələrinin gecikməsi uzaqdan müdaxilələr üçün zəmin yaradır. Bu isə o deməkdir ki, məsafədən hücumlarla mübarizə yalnız mövcud sistemləri gücləndirməklə deyil, həm də texnologiyanın dizayn mərhələsində təhlükəsizlik aspektlərinin nəzərə alınması ilə mümkündür.

Digər tərəfdən, Falco və həmkarları (2019) sənaye və istehsalat sahələrində məsafədən idarə olunan hücumların yaratdığı risklərə diqqət çəkərək, kritik infrastrukturun mühafizəsi məsələsini ön plana çıxarırlar. Onların araşdırmalarında göstərilir ki, hücumlar yalnız məlumat oğurluğu ilə məhdudlaşmır, həm də istehsalın dayanmasına, avtomatlaşdırılmış sistemlərin pozulmasına və real iqtisadi zərərlərə səbəb ola bilir. Bu isə məsafədən hücumlara qarşı milli və sektorlararası strateji yanaşmaların hazırlanmasını zəruri edir.

Bununla yanaşı, beynəlxalq təşkilatların və dövlət strukturlarının məsafədən hücumlarla bağlı siyasətləri də ədəbiyyat çərçivəsində təhlil olunur. ABŞ Müdafiə Nazirliyinin "Strategy for Operating in Cyberspace" adlı sənədində məsafədən təhdidlərin milli təhlükəsizlik üçün doğurduğu risklər qeyd olunaraq, kiberməkanın hərbi və strateji səviyyədə müdafiəsinin vacibliyi vurğulanır. Bu da göstərir ki, məsafədən hücumlarla mübarizə yalnız texniki məsələ deyil, eyni zamanda milli təhlükəsizlik siyasətinin ayrılmaz hissəsidir.

Fəxri Cəfərov (2019) Azərbaycan Respublikası Xüsusi Dövlət Mühafizə Xidmətinin əməkdaşı Fəxri Cəfərov “İnformasiya Təhlükəsizliyi” jurnalında dərc olunan məqaləsində informasiya təhlükəsizliyinin milli təhlükəsizlik sistemindəki rolunu vurğulamışdır. Məqalədə informasiya təhlükəsizliyinin təmininin fərdin, cəmiyyətin və dövlətin inkişafı üçün vacib olduğu, informasiya təhlükəsizliyinin təminatı üçün texniki və təşkilati tədbirlərin əhəmiyyəti qeyd olunmuşdur.

Müşfiq Məmmədov (2020) “Kaspersky” şirkətinin Azərbaycandakı nümayəndəsi Müşfiq Məmmədov pandemiya dövründə kiber təhlükəsizliklə bağlı sualları cavablandırarkən məsafədən hücumların artdığını və bu hücumların qarşısının alınması üçün təhlükəsizlik tədbirlərinin gücləndirilməsinin vacibliyini vurğulamışdır. O, kiber cinayətkarların fişinq, skam, DDoS hücumları, zərərli e-poçtlar və digər metodlardan istifadə etdiklərini qeyd etmişdir.

Əlizadə Mətləb Nuruş oğlu, Bayramov Hafiz Məhərrəm oğlu, Məmmədov Əlövsət Suliddin oğlu (2017). Bu müəlliflər tərəfindən yazılmış “İnformasiya Təhlükəsizliyi” dərsliyində məsafədən hücumların təhlili və mövcud müdafiə sistemləri ətraflı şəkildə izah olunmuşdur. Dərslikdə informasiya təhlükəsizliyinin əsas anlayışları, kompüter sistemlərində və şəbəkələrində informasiya təhdidləri, onların təhlili və qarşısının alınması yolları, təhlükəsizlik siyasətinin baza anlayışları və kriptoqrafik üsullarla yanaşı kompüter informasiyasının müdafiə alqoritmləri geniş şəkildə təqdim edilmişdir.

İlya Saçkov (2003-2021) O, məsafədən hücumlar, o cümlədən APT (Advanced Persistent Threat) hücumları, phishing və DDoS hücumlarına dair dərin təhlillər aparmışdır. Group-IB şirkəti Rusiya və beynəlxalq miqyasda kibercinayətkarlıqla mübarizə üzrə tanınır. Şirkətin hesabatları əsasən maliyyə sektoruna edilən uzaqdan hücumlar üzərində cəmlənmişdir.

Alisa Esage (2010-2020) O, sistem zəifliklərinin məsafədən istismarı (remote code execution) üzrə ixtisaslaşmışdır. ABŞ tərəfindən 2016-cı ildə sanksiyalara məruz qalmışdır – bu, onun fəaliyyətinin

nə qədər ciddi təsir gücünə malik olduğunu göstərir. Onun tədqiqatları əsasən Windows sistemlərindəki kritik boşluqlara fokuslanır.
Sergey Ulasen (2010) Ulasen məsafədən sənaye idarəetmə sistemlərinə (SCADA sistemlərinə) yönəlmiş zərərli proqramlar sahəsində ixtisaslaşmışdır. 2010-cu ildə Stuxnet zərərli kodunun aşkarlanması kibermühitin təhlükəsizliyi baxımından dönüş nöqtəsi hesab olunur.
Ümumilikdə, ədəbiyyat göstərir ki, məsafədən hücumlar çoxşaxəli xarakter daşıyır və onların qarşısının alınması üçün tədqiqatlar texniki, hüquqi, sosial və təşkilati aspektləri birgə əhatə etməlidir. Hücumların artan dinamikası və dəyişkən formaları, müdafiə sistemlərinin daim yenilənməsi və təkmilləşdirilməsi zərurətini doğurur. Bu baxımdan mövcud elmi yanaşmalar və texnoloji innovasiyalar məsafədən hücumlara qarşı mübarizədə əsas təməl rolunu oynayır və gələcək tədqiqatlar üçün geniş imkanlar açır.

Məqsəd

Mövzunun əsas məqsədi məsafədən hücumların mahiyyətini, bu hücumların informasiya sistemlərinə təsirini və mövcud müdafiə sistemlərinin effektivliyini araşdırmaqdan ibarətdir. Araşdırma çərçivəsində məsafədən hücumların növləri (DDoS, phishing, malware yayılması, SQL injection, remote code execution və s.), onların texniki icra mexanizmləri və tətbiq sahələri təhlil olunur. Eyni zamanda, hücumların nəticəsində yarana biləcək təhlükələr – məlumat itkisi, sistemlərin iflici, maddi və reputasiya zərərləri nəzərdən keçirilir. Mövcud müdafiə sistemləri arasında firewall-lar, antivirus proqramları, hücum aşkarlama və qarşısını alma sistemləri (IDS/IPS), şifrələmə protokolları (VPN, TLS), çoxfaktorlu autentifikasiya və süni intellektə əsaslanan təhlükə aşkarlama sistemləri kimi texnologiyaların tətbiqi və onların səmərəliliyi qiymətləndirilir. Bundan əlavə, insan faktorunun və maarifləndirmənin kibertəhlükəsizlikdə rolu qeyd olunur. Təhlükəsizlik mədəniyyəti və təşkilati siyasətlər kibermühitin qorunmasında texniki tədbirlərlə birlikdə vacib komponentlər kimi təqdim edilir. Araşdırmanın nəticələri göstərir ki, məsafədən hücumlara qarşı mübarizədə yalnız texniki həllərlə kifayətlənmək olmaz, həm də insan amilini nəzərə alan kompleks və strateji yanaşmalar vacibdir. Süni intellekt, maşın öyrənməsi və böyük verilənlərin analizi kimi innovativ texnologiyalar kibertəhlükələrə qarşı perspektivli müdafiə vasitələri kimi qiymətləndirilir. Bu baxımdan, mövzu üzrə aparılan təhlillər informasiya təhlükəsizliyinin möhkəmləndirilməsinə və effektiv müdafiə sistemlərinin formalaşdırılmasına praktiki töhfə verir.

Metodlar

Məsafədən hücumlar müasir dövrün rəqəmsal təhdidlər sistemində mühüm yer tutur. Bu hücumlar birbaşa fiziki giriş olmadan, internet vasitəsilə kompüter sistemlərinə, şəbəkələrə və verilənlər bazalarına icazəsiz müdaxilə ilə həyata keçirilir. Belə hücumlar zərərverici proqramların (malware), casus proqramların (spyware), DDoS hücumlarının, uzaqdan kod icrasının (remote code execution), və sosial mühəndislik metodlarının tətbiqi ilə gerçəkləşir. Təhlil göstərir ki, bu hücumlar əksər hallarda sistemdəki zəifliklərdən, istifadəçilərin məlumat azlığından və təşkilatların təhlükəsizlik siyasətindəki boşluqlardan istifadə etməklə həyata keçirilir.
Bu tip hücumların ən geniş yayılmış formalarından biri DDoS hücumlarıdır. Bu zaman hücum edən tərəf bir neçə min cihazı nəzarət altına alaraq hədəf sistemə eyni anda çoxsaylı müraciət göndərir və nəticədə sistemin işləməsi dayanır. Eyni zamanda, “remote access Trojan” (RAT) və “keylogger” kimi proqramlar vasitəsilə istifadəçi fəaliyyətləri izlənilir və parollar oğurlanır. Bu cür hallar xüsusilə bank sistemləri, dövlət orqanları, səhiyyə və təhsil infrastrukturları üçün ciddi təhlükələr yaradır.
Təhlilin digər mühüm tərəfi mövcud müdafiə sistemlərinin imkanları və məhdudiyyətləridir. Müasir təhlükəsizlik sistemləri bir neçə səviyyədən ibarətdir: şəbəkə səviyyəsində firewall-lar və IDS/IPS sistemləri, tətbiq səviyyəsində antivirus və antimalware proqramları, istifadəçi səviyyəsində isə çoxfaktorlu autentifikasiya və davranış monitorinq sistemləri. Bu texnologiyalar müəyyən səviyyəyə qədər effektivlik təmin etsə də, hücum texnikalarının sürətlə dəyişməsi və təkmilləşməsi səbəbindən onlar tez köhnəlmiş olur və yeni risklər qarşısında zəif qalır.

Süni intellektin və maşın öyrənməsi modellərinin təhlükə aşkarlama sistemlərinə inteqrasiyası bu sahədə inqilabi dəyişikliklər vəd edir. Bu texnologiyalar istifadəçi davranışlarını və şəbəkə anomaliyalarını real vaxtda təhlil edərək potensial təhlükələri əvvəlcədən proqnozlaşdırmağa və cavab verməyə imkan yaradır. Bu da klassik metodların sərhədlərini aşaraq adaptiv müdafiə yanaşmalarının tətbiqini aktuallaşdırır. Eyni zamanda, məsafədən hücumların hüquqi və etik aspektləri də təhlilin ayrılmaz hissəsidir. Hücum edənlərin əksəriyyəti beynəlxalq miqyasda fəaliyyət göstərdiyindən hüquqi məsuliyyətin müəyyənləşdirilməsi və hücumların mənbəyinin aşkarlanması çətinləşir. Bu baxımdan beynəlxalq əməkdaşlıq, hüquqi standartlaşdırma və məlumat mübadiləsi zərurətə çevrilmişdir.

Mövzunun daha dərin təhlili göstərir ki, məsafədən hücumların artması təkcə texnoloji inkişafın nəticəsi deyil, həm də rəqəmsal təhlükəsizlik strategiyalarında olan gecikmələrin və boşluqların nəticəsidir. Bu cür hücumların çoxu zəif şifrələnmiş sistemlərə, vaxtında yenilənməyən proqram təminatına və qeyri-kafi istifadəçi nəzarətinə əsaslanır. Bu səbəbdən, təşkilatlar sadəcə texniki müdafiə tədbirləri ilə kifayətlənməməli, eyni zamanda təhlükəsizlik siyasətlərini təkmilləşdirməli, risklərin qiymətləndirilməsi və idarə olunması mexanizmlərini gücləndirməlidirlər. Bir çox hallarda məsafədən hücumların əsas hədəfi kritik infrastruktur obyektləri olur. Enerji sistemləri, nəqliyyat şəbəkələri, su təchizatı və səhiyyə informasiya sistemləri hücumların xüsusi diqqət göstərdiyi sahələrdir. Bu obyektlərin fəaliyyətində yaranan fasilələr yalnız texniki problemlərlə deyil, həm də ictimai panika və iqtisadi zərərlərlə müşayiət olunur. Belə halların qarşısını almaq üçün milli təhlükəsizlik səviyyəsində inteqrasiya olunmuş kibertəhlükəsizlik planlarının hazırlanması və tətbiqi zəruridir.

Təhlil göstərir ki, məsafədən hücumların qarşısını almaqda istifadəçi maarifləndirilməsi ən az texniki müdafiə sistemləri qədər əhəmiyyətlidir. Bir çox hücumlar istifadəçilərin e-poçtla göndərilən zərərli keçidlərə klikləməsi və ya sosial mühəndislik vasitəsilə öz məlumatlarını təqdim etməsi nəticəsində baş verir. Bu baxımdan təhlükəsizlik üzrə təlim proqramları, məlumatlılıq kampaniyaları və real ssenarilər əsasında keçirilən simulyasiyalar təşkilatların davamlı müdafiə qabiliyyətini artırır. Texnologiyanın inkişafı ilə paralel olaraq məsafədən hücumların formaları da getdikcə mürəkkəbləşir. Artıq "Advanced Persistent Threats" (APT) kimi uzunmüddətli və hədəfə yönəlmiş hücumlar geniş yayılmaqdadır. Bu hücumlar sistemə dərhal zərər yetirmək əvəzinə, aylar və ya illərlə gizli şəkildə fəaliyyət göstərərək dəyərli məlumatların ötürülməsi və ya sabotaj məqsədilə istifadə olunur. Belə təhdidlərə qarşı ənənəvi üsullar kifayət etmədiyindən, davranış əsaslı analiz, süni intellekt texnologiyaları və adaptiv müdafiə sistemləri vacib alətlərə çevrilmişdir.

Sonda qeyd etmək lazımdır ki, məsafədən hücumların təhlili yalnız mövcud vəziyyətin qiymətləndirilməsi üçün deyil, həm də gələcək risklərin qabaqlanması və proaktiv müdafiə strategiyalarının qurulması üçün əsaslı baza yaradır. Bu təhlil göstərir ki, kibertəhlükəsizlik sahəsində uğur qazanmaq üçün texnologiya, insan resursları və hüquqi çərçivə arasında balanslı və koordinasiyalı yanaşma tələb olunur. Təkamül edən kibertəhlükələrlə effektiv mübarizə yalnız kompleks və davamlı inkişaf edən müdafiə mexanizmləri ilə mümkündür.

Bununla yanaşı, məsafədən hücumların artan miqyası dövlətlərin və beynəlxalq təşkilatların da bu sahəyə diqqətini cəlb etmişdir. Birləşmiş Millətlər Təşkilatı, NATO, Avropa İttifaqı kimi qurumlar kibertəhlükəsizliyi qlobal təhlükəsizlik konsepsiyasının ayrılmaz hissəsi kimi qəbul edir və ölkələr arasında informasiya təhlükəsizliyi üzrə əməkdaşlıq mexanizmləri qurmağa çalışırlar. Məsafədən hücumlar sərhəd tanımadığı üçün onların qarşısının alınması da yalnız milli səviyyədə deyil, beynəlxalq koordinasiya və təcrübə mübadiləsi əsasında mümkün olur. Bu baxımdan, Azərbaycanın da bu prosesə inteqrasiya olunması və beynəlxalq kibertəhlükəsizlik standartlarına uyğun müdafiə strukturlarını inkişaf etdirməsi zəruridir.

Tədqiqatlar onu da göstərir ki, məsafədən hücumlara qarşı effektiv cavab tədbirlərinin hazırlanması üçün kiberinsidentlərin qeydiyyatı və təhlilinin sistemli şəkildə aparılması mühümdür. Bu məqsədlə Computer Emergency Response Team (CERT) və Security Operation Center (SOC) kimi qurumların rolu xüsusi əhəmiyyət kəsb edir. Belə qurumlar real vaxtda təhdidlərin monitorinqini aparır, insidentlərə cavab verir və gələcək hücumların qarşısını almaq üçün analitik hesabatlar hazırlayırlar. Digər mühüm məsələ isə məsafədən hücumlara qarşı sınaq mühitlərinin yaradılmasıdır. "Penetration testing" (sızma testləri) və "Red Team" ssenariləri təşkilatlara öz sistemlərinin zəif nöqtələrini

müəyyən etməyə və real hücum şəraitində davranışlarını təkmilləşdirməyə imkan verir. Bu cür testlər kibermüdafiə hazırlığının artırılması üçün mühüm əhəmiyyət daşıyır və qabaqlayıcı tədbirlərin effektivliyini yüksəldir.

Nəticə

Məsafədən hücumların təhlili və mövcud müdafiə sistemlərinin araşdırılması göstərir ki, rəqəmsal təhlükəsizlik müasir informasiya cəmiyyətinin ən vacib istiqamətlərindən birinə çevrilmişdir. Bu tip hücumlar texniki zəifliklərlə yanaşı, insan faktoru və təşkilati boşluqlardan da istifadə edərək ciddi risklər yaradır. Hücumların artan miqyası və mürəkkəbliyi informasiya sistemlərinin daha güclü və çoxsəviyyəli müdafiə sistemləri ilə təchiz olunmasını zəruri edir. Ənənəvi təhlükəsizlik yanaşmaları artıq təkbaşına kifayət etmir, ona görə də süni intellekt, maşın öyrənməsi, davranış analizləri və avtomatlaşdırılmış monitorinq sistemlərinin tətbiqi bu sahədə yeni imkanlar açır.

Eyni zamanda, məsafədən hücumlara qarşı mübarizədə beynəlxalq əməkdaşlıq, hüquqi tənzimləmələrin gücləndirilməsi və mütəmadi maarifləndirmə tədbirləri xüsusi önəm daşıyır. Təşkilatların kibertəhlükələrə qarşı hazırlıq səviyyəsi yalnız texniki vasitələrlə deyil, həm də proaktiv strategiyalar, insident menecmenti və kadr potensialı ilə müəyyən olunur. Təhlükəsizlik mədəniyyətinin formalaşdırılması və təhlükə idarəetmə sistemlərinin qurulması məsafədən hücumların təsirini minimuma endirmək üçün əsas şərtdir.

Bu təhlil nəticəsində gəlinən qənaət ondan ibarətdir ki, məsafədən hücumlarla effektiv mübarizə yalnız kompleks, çevik və adaptiv yanaşmalarla mümkündür. İnnovativ texnologiyalarla yanaşı, normativ-hüquqi bazanın gücləndirilməsi, milli təhlükəsizlik strategiyalarının təkmilləşdirilməsi və beynəlxalq səviyyədə koordinasiya bu sahədə uğur qazanmaq üçün əsas amillərdir. Beləliklə, məsafədən hücumların qarşısının alınması və kibertəhlükəsizlik sahəsində davamlı inkişafın təmin olunması üçün çoxşaxəli və sistemli fəaliyyət strategiyası həyata keçirilməlidir.

ƏDƏBİYYAT

1. Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0130-PMC
2. Falco, G., Caldera, C., & Shrobe, H. (2019). Cybersecurity risk in advanced manufacturing. *Journal of Cybersecurity*, *5*(1), tyz007. https://doi.org/10.1093/cybsec/tyz007
3. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10. https://doi.org/10.3233/THC-161263
4. Lee, I., & Lee, K. (2020). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *63*(4), 431–440. https://doi.org/10.1016/j.bushor.2020.03.-005
5. Loukas, G., Oke, G., & Vuong, T. (2013). A taxonomy and survey of cyber threats and defense mechanisms for emergency management systems. *ACM Computing Surveys*, *45*(4), 1–36. https://doi.org/10.1145/2501654.2501656PMC
6. Maleks Smith, J., Sheehan, M., & Biener, C. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *Journal of Cybersecurity*, *8*(1), tyac001. https://doi.org/10.1093/-cybsec/tyac001PMC
7. Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1), tyz002. https://-doi.org/10.1093/cybsec/tyz002PMC
8. Ulven, J., & Wangen, G. (2021). Cybersecurity risk in higher education institutions: A systematic review. *Computers & Security*, *102*, 102131. https://doi.org/10.1016/j.cose.2020.102131PMC
9. U.S. Department of Defense. (2011). *Strategy for Operating in Cyberspace*. https://en.wikipedia.org/wiki/U.S._Department_of_Defense_Strategy_for_Operating_in_CyberspaceVikipedi

ISSN: 1609-1620
VOLUME 27 ISSUE 06 2025

10. Zhou, Y., & Leung, H. (2023). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Electronics*, *12*(6), 1333. https://doi.org/10.-3390/electronics12061333ResearchGate

АНАЛИЗ ДИСТАНЦИОННЫХ АТАК И СУЩЕСТВУЮЩИХ СИСТЕМ ЗАЩИТЫ

РЕЗЮМЕ

Вагиф Каримов[1], Джаббар Гасанов[2]
[1,2]Азербайджанский государственный университет нефти и промышленности
[1]Кафедра «Общаяй и прикладная математика»
[2]Кафедра «Компьютерная инженерия»
[1]Доцент, кандидат технических наук, kvaqif56@gmail.com
[2]Студент-магистр, cabbarhesenov1999@gmail.com

Удаленные атаки являются одной из самых серьезных угроз кибербезопасности в сфере информационных технологий. Эти атаки осуществляются без прямого физического контакта, через Интернет или другие сетевые каналы. С ростом числа удаленных атак возникла необходимость в постоянном обновлении стратегий кибербезопасности. Из-за гибкости и сложности векторов атак одних традиционных механизмов защиты недостаточно. По этой причине на первый план выходят проактивные подходы к обеспечению безопасности, то есть методы выявления и снижения рисков до атаки. Поскольку фишинговые и социально-инженерные атаки в основном эксплуатируют человеческие слабости, меры по повышению осведомленности в этой области так же важны, как и технические меры. Среди инновационных подходов особенно выделяются системы на основе искусственного интеллекта (ИИ) и машинного обучения (МО). Таким образом, атаки, осуществляемые из внутренней сети, предотвращаются более эффективно. Важную роль в развитии данной сферы играют также нормативно-правовая база и стандарты, принятые на государственном и международном уровнях. Например, законодательство о защите данных, такое как GDPR (Общий регламент Европейского союза по защите данных), обязывает организации принимать более строгие меры безопасности. Такого рода правила служат для обеспечения безопасности киберсреды, определяя не только технические, но и этические и правовые рамки.
Ключевые слова: удаленные атаки, кибербезопасность, системы защиты, удаленное выполнение кода, системы обнаружения вторжений (IDS/IPS).

Publishing history: 30.06.2025
Article received: 22.05.2025
Article accepted: 10.06.2025