UOT 004.056 DOI: 10.25045/jpit.v12.i2.02

İmamverdiyev Y.N.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@iit.science.az

SƏNAYE İDARƏETMƏ SİSTEMLƏRİNDƏ KİBERTƏHLÜKƏSİZLİK PROBLEMLƏRİNİN ANALİZİ

Daxil olmuşdur: 26.04.2021 Düzəliş olunmuşdur: 02.05.2021 Qəbul olunmuşdur: 18.05.2021

Sənaye idarəetmə sistemləri (SİS) elektrik istehsalı və təchizatı, içməli su təchizatı, neft və neft-kimya, nüvə enerjisi, nəqliyyat sistemləri, dəmir yolu və metro sistemlərində idarəetmə və monitorinq üçün geniş istifadə olunurlar. Onlar bu kritik milli infrastrukturlarda əməliyyatların beyni və onurğa sütunudur. Kritik infrastrukturların işinin pozulması cəmiyyətə sürətlə və getdikcə kəskinləşən təsir göstərə bilər və bu təsiri kritik infrastrukturlar arasında yüksək dərəcədə qarşılıqlı asılılıq daha da ağırlaşdırır. 2009-cu ildə aşkarlanmış Stuxnet zərərli proqramı SİS kibertəhlükəsizliyinin reallığını və ciddiliyini göstərdi. Industry 4.0 konsepsiyasının geniş tətbiqi ilə əlaqədar SİS-lərin kibertəhlükəsizliyi xüsusi aktuallıq kəsb edir. Məqalədə SİS-lərin mahiyyəti və komponentləri barədə qısa məlumat verilir və onların kibertəhlükəsizliyinin müasir vəziyyətinin qısa analizi aparılır. SİS-lərin kibertəhlükəsizliyinin qiymətləndirilməsi üzrə tədqiqatlar risklərin idarə edilməsi, zərərli proqram təminatının aşkarlanması və analizi metodları, kibertəhlükəsizliyin monitorinqi üçün honeynet texnologiyaları və test stendlərinin yaradılması istiqamətləri üzrə analiz edilir və hər bir istiqamət üzrə açıq tədqiqat problemləri göstərilir. Əsas tədqiqat metodları modelləşdirmə, müqayisəli və təsviri metodlar, analogiya, analiz və sintez metodlarıdır; əsas tədqiqat yanaşmaları sistemli, kompleks və situativ yanaşmadır. Alınmış nəticələrin ölkədə SİS-lərin kibertəhlükəsizliyi infrastrukturunun formalaşdırılması və inkişafında, SİS kibertəhlükəsizliyi sahəsində elmi tədqiqatların təkmilləşdirilməsi və milli informasiya təhlükəsizliyi üzrə tədbirlər kompleksinin işlənməsində və praktiki reallaşdırılmasında faydalı olacağı gözlənilir.

Açar sözlər: *sənaye idarəetmə sistemi, SCADA, PLC, kritik milli infrastruktur, kibertəhlükəsizlik.*

Giriş

Industry 4.0 konsepsiyasının geniş tətbiqi ilə əlaqədar SIS-lərin (*ing. ICS, Industrial Control Systems,)* kibertəhlükəsizliyi xüsusi aktuallıq qazanır [1]. SİS ümumi termindir, dispetçer nəzarəti və verilənlərin toplanması sistemləri (*ing.Supervisory Control And Data Acquisition, SCADA*), paylanmış idarəetmə sistemləri (*ing. Distrubuted Control System, DCS*), prosesləri idarəetmə sistemləri (*ing. Process Control System, PCS*) və proqramlanan məntiqi kontrollerlər (*ing. Programmable Logic Controller, PLC*) kimi konfiqurasiyaları əhatə edir [2]. SİS bir çox kritik milli infrastrukturun əsasını təşkil edir. Neft-kimya sənayesi, atom elektrik stansiyaları (AES), elektrik təchizatı, su təchizatı qurğuları, metro və s. kimi əsas infrasrukturlar SİS olmadan normal işləyə bilməz.

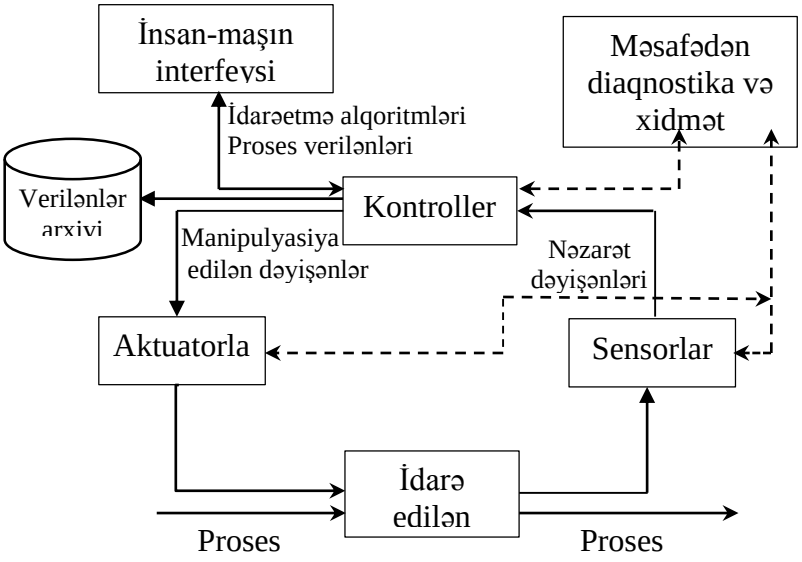
Müasir informasiya və kommunikasiya texnologiyalarının (İKT) inkişafı SİS-lərin dizaynında da inqilab etmişdir. SIS-lərdə ənənəvi elektromexaniki sistemlərdən rəqəmsal şəbəkə sistemlərinə əhəmiyyətli keçid baş vermişdir və İnternet üzərindən ən yeni informasiya texnologiyalarının köməyi ilə idarə edilən fiziki proseslər arasında güclü bir interfeys yaranmışdır [2]. Aktuatorlar və sensorlar kimi aparat və proqram komponentlərinin və fiziki proseslərin mürəkkəb şəkildə birləşməsi ilə kritik infrastrukturlar *SCADA, PLC, DCS* və s. kimi kontrollerlər əsasında monitorinq və idarə edilir. Bu texnologiyaların inteqrasiyası xarici mühitdən SİS-ə girişi əhəmiyyətli dərəcədə asanlaşdırır. Digər tərəfdən, bu, bir çox kritik kibertəhlükəsizlik problemlərinə də gətirib çıxarır [3]. Bu problemlərin xarakteri elədir ki, düzgün idarə edilmədikdə, onların milli iqtisadiyyat üçün istehsal itkiləri şəklində arzuolunmaz nəticələri ola bilər, bəzən insan sağlığına və ətraf mühitin təhlükəsizliyinə də ciddi təhdidlər yarana bilər [4].

SİS-in əsas komponentləri

Avtomatlaşdırılmış idarəetmə sistemlərinin reallaşdırılması müxtəlif sənaye prosesləri üçün fərqli cəhətlərə malik ola bilər, lakin şəkil 1-də göstərilən ümumi arxitektura gözlənilir.

Bu arxitekturanın əsas komponentləri aşağıdakılardır [2]:

- **İdarəetmə konturu** klapanlar, çeviricilər və mühərriklər kimi *aktuatorlardan*, sənaye prosesi ilə əlaqəli vəziyyət dəyişənlərini (məsələn, temperatur, təzyiq, axın sürətləri) müəyyən edən *sensorlardan* və sensor göstəriciləri və operator daxiletməsi əsasında aktuatorları idarə edən *kontrollerdən* ibarətdir.
- **İnsan-maşın interfeysi** (İMİ) operatorlara idarə edilən prosesə nəzarət etməyə və ona təsir etməyə imkan verir.
- **Verilənlərin arxivatoru** proses idarəetməsi üzrə bütün hərəkətləri qeydə alır, bir neçə səviyyədə məlumat verməyə imkan verir.
- **Məsafədən diaqnostika və xidmət** əməliyyat problemlərinin diaqnostikası və korreksiyası üçün giriş imkanı verir.



Şəkil 1. SİS komponentləri.

Tipik SİS şəbəkə protokolları stekindən istifadə edilməklə qurulmuş bir neçə idarəetmə konturundan, maşın-insan interfeyslərindən və məsafədən diaqnostika/xidmət alətlərindən ibarətdir. Müasir SİS-lər Modbus/TCP, DNP3, Ether/IP və Profibus kimi tətbiqi səviyyə kommunikasiya protokollarından istifadə edirlər [5].

SİS-in sahə qurğuları ilə qarşılıqlı təsirdə olan əsas komponenti *PLC*-dir. Qeyd edək ki, İlk *PLC* 1968-ci ildə yaradılmışdı. 1950-ci illərdə idarəetmə rele sxemlərinin köməyi ilə reallaşdırılırdı.

Müasir SİS-lərdə diskret və ya analoq sensorları istifadə edilir. Sahə məlumatlarını sensorlardan idarəetmə sisteminə daxil etmək üçün elektrik siqnalları rəqəmləşdirilməlidir. Bunu *RTU* (*ing. Remote Terminal Unit*), *PLC, IED* (*ing. Intelligent Electronic Device*) kimi avadanlıqlar istifadə edilməklə etmək olar [2].

SİS-lərdə kibertəhlükəsizliyin bəzi xüsusiyyətləri

SİS-lərin kibertəhlükəsizliyi problemi son 10 ilə kimi aktual deyildi. Problemə maraq sənaye obyektlərinə hücum edən viruslarla əlaqəli insidentlərdən sonra yarandı [6]. Əvvəllər hesab olunurdu ki, SİS-in işinə müdaxilə etmək olduqca çətindir. Belə təsəvvür bir neçə postulata əsaslanırdı: hər bir SİS-in proqram təminatı unikaldır və qapalıdır; SİS lokal şəbəkəsi girişin idarə olunması problemini həll edir; SİS-ə sızmaq böyük xərclərlə bağlıdır və nəticədə nə əldə ediləcəyi aydın deyil.

Zərərli proqramlar SİS komponentlərindəki boşluqlardan fəal istifadə edirlər. Stuxnet və Flame kimi insidentlər SİS təhlükəsizliyinin təmin edilməsi məsələlərinə diqqəti cəlb etdilər [7, 8]. Stuxnet, Siemens şirkətinin istehsal etdiyi *PLC* sistemlərinə kiberhücumlar həyata keçirən zərərli proqram təminatıdır.

SİS-lərin əhəmiyyəti və təbiəti onların davamlı təhlükəsizliyini təmin etmək üçün xüsusi çətinliklər yaradır. SİS təhlükəsizlik vəziyyətinin araşdırılması olduqca narahatedici bir mənzərəni aşkara çıxarır. Aşkarlanan boşluqların sayı artır və hər beş boşluqdan biri bir aydan çox müddətə aradan qaldırılır. Boşluqların yarısı hakerlərə zərərli kodu işə salmağa imkan verir [5, 6].

SİS-in xarakterik xüsusiyyəti korporativ şəbəkələrdən təcrid olunması idi, bu da xarici təhdidlərdən tələb olunan təhlükəsizlik səviyyəsini təmin edirdi. Bu gün resursların, korporativ şəbəkə xidmətlərinin və SİS-in müəssisə menecmentinin ümumi şəbəkəsinə inteqrasiya prosesi müşahidə edilir. Həm də, SİS şəbəkəsini müəssisə şəbəkələrindən fərqləndirən vacib cəhətləri qeyd etmək lazımdır [2, 7]:

- Keçmişdə proses idarəetmə şəbəkələri onları digər daxili və xarici sistemlərdən ayıran "hava boşluğu" ilə effektiv şəkildə qorunurdu; bu, ümumiyyətlə, artıq belə deyil və indi onu mürəkkəb qaydalar çoxluğu olan şəbəkə ekranları əvəz edir.
- *SCADA* sistemləri sahə qurğularının fiziki təhlükəsizliyi məhdud olan və coğrafi baxımdan yüzlərlə kilometr məsafələrdə paylanmış sistemlərdir. Bir çox SİS komponenti (xüsusən uzaq telemetriya qurğuları) təhlükəsizlik xüsusiyyətləri məhdud və istehsalçı tərəfindən yenilənmələri az perspektivli olan köhnə qurğulardır.
- SİS fasiləsiz (gecə-gündüz) onlayn rejimdə işləyir, bu, onun proqram-aparat kompleksinin vaxtında yenilənməsinə və sınaqdan keçirilməsinə mane olur; texnoloji şəbəkələrdə sistemin imtinası və ya işləməməsi kritikdir;
- Təhlükəsizlik yenilənmələrinin menecmenti böyük problemdir, çünki əməliyyat sistemi (ƏS) və ya tətbiqdə edilmiş dəyişikliklərin gözlənilməz yan təsirləri nəticəsində SİS-in işinin pozulması riskinin qarşısını almaq üçün minimum dəyişikliklər edilməlidir.
- Şəbəkə protokolları adətən autentifikasiya olunmur və verilənlər açıq mətnlə ötürülür.
- Qapalı, məxfi protokollardan və ƏS-lərindən açıq kodlu və ya hazır kommersiya texnologiyasına miqrasiya o deməkdir ki, arxitektura haqqında sənədləşdirilmiş məlumatları daha asanlıqla əldə etmək olar.
- Əsas tələb fasiləsiz və düzgün funksiya olduğundan, bunları pozmaq riski olan bir çox təhlükəsizlik mexanizmlərinə yol verilmir; məsələn, pis parollar təkrarlandıqda, antivirus proqramı və ya IDS/IPS tərəfindən operatorun bloklanması və s. çox vaxt həyata keçirilə bilməz.
- Əhəmiyyətli resursları olan dövlətlər düşmənlərinin kritik milli infrastrukturuna aid sistemlərdə zəif cəhətləri tapmaq və istismar etmək üçün xeyli vəsait xərcləməyə hazırdırlar.

Mövcud icmalların analizi

2009-cu ildə Stuxnetin aşkarlanmasından sonra SİS-lərin kibertəhlükəsizliyi tədqiqatçıların diqqətini xüsusilə cəlb etmişdir və bu mövzuda bir sıra icmal məqalələri çap olunmuşdur. Aşağıda onların qısa icmalı verilir.

SİS kibertəhlükəsizliyinin geniş mənzərəsi [10]-da ətraflı analiz edilir, o cumlədən: 1) SİS-in əsas prinsipləri və unikal aspektləri; 2) SİS-ə kiberhücumların qısa tarixi; 3) SİS təhlükəsizliyinin qiymətləndirilməsinə dair icmal; 4) SİS-in müxtəlif səviyyələri arasındakı qarşılıqlı əlaqələri qeydə alan test-stendlərinin icmalı; 5) SİS-ə hücumlar və müdafiə sahəsində hazırkı tendensiyalar araşdırılır.

SİS-in kibertəhlükəsizliyinin vəziyyəti və kibertəhlükəsizlik sistemlərində tətbiq olunan əsas metodlar [11]-də nəzərdən keçirilir, SİS-in kibertəhlükəsizliyi üçün çağırışlar və gələcək tədqiqat istiqamətləri təsvir olunur.

SİS-lərin avtonom sistemlərdən bulud mühitlərinə keçməsinə [12]-də ətraflı baxılır. Etibarlı SİS-lərin yaradılması üzrə əsas işlər, xüsusən də SİS-lərin kibertəhlükəsizliyi üçün maşın öyrənmə metodlarının tətbiqi müzakirə edilir. Bu, sənaye proseslərinin, xüsusilə də bulud mühitinə keçərkən təhlükəsizliyinin təmin edilməsi problemlərini həll etməyə kömək edə bilər.

SİS-lərə mümkün kiberhücumlar [13]-də nəzərdən keçirilir, tipik təhdidlər və boşluqlar müəyyənləşdirilir və SİS-lərin kibermüdafiəsi (məsələn, risk qiymətləndirmə metodologiyalarının köməyi ilə) və digər müdafiə tədbirləri müzakirə edilir. SİS-lərin kibertəhlükəsizliyində açıq tədqiqat problemləri də müəyyənləşdirilir, güclü və zəif tərəflərini göstərməklə mövcud təhlükəsizlik həlləri təsnif edilir.

SİS-lərə son 20 ildə edilmiş böyük hücumların icmalı [14]-də verilir. Məqalədə vurulmuş iqtisadi zərər, fiziki avadanlığın məhv edilməsi və potensial insan itkiləri baxımından fərqlənmiş hücumlar seçilmişdir. Bu hücumların hər biri üçün istifadə edilmiş metodologiya təsvir olunur və onların qarşısının alınması üçün mümkün həllər təklif edilir. SİS-lərin təhlükəsizliyi üçün ən yaxşı müdafiə metodları üzrə bəzi tövsiyələr verilir.

Davamlı təkmil hücumlar (*ing. Advanced Persistent Threats, APT*) hər bir kritik infrastruktur üçün ciddi təhdidə çevrilmişdir, çünki bu mürəkkəb hücumlardan bütün sənaye aktivlərinin müdafiəsi üçün vahid həll mövcud deyil. Hansı müdafiə mexanizmlərinin birinci müdafiə xətti kimi istifadə ediləcəyini də başa düşmək vacibdir. Bu məqsədlə [15]-də *APT*-nin sənaye ekosisteminin mövcud və yeni elementlərinə qarşı istifadə edə biləcəyi hücum vektorlarının spektri öyrənilir. Daha sonra müdaxilələrin aşkarlanması sistemlərinin (i*ng. Intrusion Detection Systems, IDS*) evolyusiyası və SİS-lərdə tətbiqi imkanları analiz edilir.

Müəlliflər [16]-da SİS-in kibertəhlükəsizliyi problemlərinin unikal aspektlərinin hərtərəfli icmalını verməyə cəhd edirlər. O cümlədən, SİS-in təhlükəsizliyinin qiymətləndirilməsi və arxitekturasının analizi məsələlərinə daha dərindən baxılır. SİS-ə müxtəlif hücumların qısa icmalı da verilir.

Bu məqalədə təqdim olunan icmal aşağıdakı istiqamətlər üzrə aparılmışdır:

- SİS-lərdə kibertəhlükəsizlik risklərinin qiymətləndirilməsi metodları;
- SİS-lərdə zərərli proqram təminatının aşkarlanması və analizi metodları;
- SİS-lərdə kibertəhlükəsizliyin monitorinqi və hücumların aşkarlanması metodları;
- SİS-lərin kibertəhlükəsizliyi üçün *honeypot* yanaşmaları;
- SİS-lərin kibertəhlükəsizliyinin qiymətləndirilməsi üçün test stendləri.

SİS-lərdə kibertəhlükəsizlik risklərinin qiymətləndirilməsi metodları

SİS-lərdə kibertəhlükəsizlik risklərinin ölçülməsi və idarə edilməsi sahəsində ən yeni metodologiyalara və tədqiqatlara [17]-də baxılır. SİS-lər üçün spesifik olan təhlükəsizlik metrikalarının yoxluğu bu metodologiyaların tətbiqinə əsas manea kimi identifikasiya edilir. Buna görə, SİS-lərin təhlükəsizlik metrikaları üzrə gələcək tədqiqat planları təklif edilir. İmtinalara dayanıqlı SİS əməliyyatları üçün "funksional zəmanət" konsepsiyası da daxil edilir.

Təhlükəsizlik risklərini SİS-lərin həyat tsiklinin bütün mərhələlərində – layihələndirmədən başlamaqla istismardan çıxarılmağa qədər idarə etmək zəruridir. Risklərin qiymətləndirilməsi risklərin idarə olunmasının ayrılmaz tərkib hissəsidir. Bu baxımdan risklərin kəmiyyət qiymətləndirilməsi həyati vacibdir, çünki kiber risklərin ölçülməsi təhlükəsizliyə investisiyalar üzrə effektiv qərar qəbuletmə proseslərinin yaradılması üçün olduqca zəruridir. SİS üçün təhlükəsizlik risklərinin kəmiyyət qiymətləndirilməsi sahəsində işlərin vəziyyətinə [18] icmal məqaləsində baxılır və gələcək tədqiqatlar və əlaqəli problemlər üçün vədedici imkanlar müəyyənləşdirilir. SİS üçün təhlükəsizlik risklərinin kəmiyyət qiymətləndirilməsinin müasir vəziyyətinin SİS-in xüsusiyyətlərinə uyğunlaşdırılmış adekvat (dinamik) risk qiymətləndirilməsi metodlarının olmaması ilə xarakterizə olunduğu vurğulanır. Sənaye 4.0 işığında təhdidlərin mürəkkəbliyinin artması və təhlükəsizlik hadisələri ilə əlaqəli tarixi məlumatların olmaması onu daha da ağırlaşdırır.

SCADA sistemlərdə kibertəhlükəsizlik risklərinin qiymətləndirilməsi yanaşmaları [19]-da nəzərdən keçirilir. *SCADA* sistemlərinə tətbiq üçün işlənmiş 24 risk qiymətləndirmə metodu seçilir və ətraflı araşdırılır. Metodların mahiyyəti təsvir edilir və sonra məqsəd, tətbiq sahəsi, risklərin idarə olunması mərhələləri, ehtimal verilənlərinin mənbələri və s. baxımından analiz edilir. Analizə əsasən, *SCADA* sistemləri üçün kibertəhlükəsizlik riskinin qiymətləndirilməsi metodlarının kateqoriyalaşdırılması üçün intuitiv sxem təklif edilir.

Cihazların rəqəmsallaşdırılması və şəbəkələşməsinin davamlı inkişafı ilə, atom elektrik stansiyalarındakı (AES-lərdəki) SİS-lərin kibertəhlükəsizliyi misli görünməmiş problemlərlə üzləşir. Buna görə, AES-lərin kibertəhlükəsizliyini planlaşdırma və tikinti mərhələsindən başlayaraq nəzərə almaq lazımdır [20]. Məqalədə kibertəhlükəsizlik riskləri tikinti mərhələsində analiz edilir, əlaqəli standartları və qaydaları birləşdirərək yeni tikilən və tikiləcək AES-lər üçün texniki müdafiə arxitekturaları təklif edilir. Nəhayət, müdafiə arxitekturasının məqsədəuyğunluğunu yoxlamaq üçün rəqəmsal əkizlər əsasında SİS-lərin kibertəhlükəsizliyinin test platformalarının qurulması təklif edilir.

Hədəfə alınan idarəetmə sisteminin davranışını dəyişən kiberhücumların idarə edilən fiziki sistem haqqında biliklərdən istifadə etməklə aşkarlanması [21]-də göstərilir. Fiziki sistem haqqında biliklərdən istifadə edərək, diqqəti boşluqların istismarının konkret mexanizmlərində deyil, hücumun son məqsədində cəmləmək olar. Təhlükəsizlik mexanizmlərinin təhlükəsizliyi və etibarlılığı gizli hücumların təsirləri tədqiq olunmaqla və hücuma avtomatik reaksiya mexanizmlərinin sistemi təhlükəsiz olmayan vəziyyətə gətirməyəcəyinə zəmanət verməklə qiymətləndirilir.

Hazırda təhlükəsizlik və sağlamlıq riskləri ayrılıqda analiz edilir. Lakin bu, yanlışdır, çünki təhlükəsizlik təhdidi də sağlamlıq insidenti kimi eyni təhlükəli hadisələrə səbəb ola bilər. [22]-də sənayedə risk analizi zamanı təhlükəsizlik və insan sağlığı risklərinə bir yerdə baxan yeni metod təklif olunur. Bu yanaşma, adətən, təhlükəsizlik analizi üçün istifadə edilən «kəpənək» tipli analizi hücum ağacları analizinin SİS-lərin təhlükəsizliyi üçün genişləndirilmiş versiyası ilə birləşdirir. «Kəpənək» ilə hücum ağaclarının birlikdə istifadəsi təhlükəsizlik baxımından risk senarilərinin ətraflı təsvirini təmin edir. Daha sonra risk səviyyəsini qiymətləndirmək üçün ehtimalın biri təhlükəsizlik, digəri isə insan sağlığı üçün olmaqla iki komponentinə əsaslanaraq yanaşma təklif edilir. Bu yanaşmanın tətbiqi kimya müəssisəsində bir risk senarisi misalında nümayiş etdirilir.

Təhlükəsiz SİS-lərin yaradılması üzrə tövsiyələr [23]-də öz əksini tapır. Sənəddə SİS-in qısa icmalı verilir, sistemlərin tipik topologiyaları və arxitekturalarına baxılır, bu sistemlər üçün tipik təhdidlər və boşluqlar müəyyən edilir, həmçinin əlaqədar risklərin azaldılması üçün tövsiyə edilən təhlükəsizlik tədbirləri təklif edilir.

SİS-lərdə zərərli proqramların aşkarlanması və analizi metodları

SİS-lərdə kibertəhlükəsizliyin təmin edilməsinin əsas məsələlərindən biri bu sistemlərdə istifadə edilən proqram təminatının təhlükəsizliyinin təmin edilməsi məsələsidir. Bu məsələ həmin sistemlərdə müxtəlif proqram və aparat təminatının istifadəsi ilə şərtlənən icra mühitinin heterogenliyi və spesifik şəbəkə protokollarının tətbiqi ilə daha da mürəkkəbləşir.

Zərərli proqramların aşkarlanmasında ən çox iki üsul tətbiq olunur: statik və dinamik analiz [24]. Statik analiz əlamətləri çıxarmaq məqsədi ilə proqramın binar kodunu assembler kodduna çevirərək onun sintaksisini və struktur xassələrini istifadə edir. Dinamik analiz isə, icra zamanı xarakterik hərəkətlərini müəyyən etmək üçün proqram yerinə yetirilməklə aparılır. Tədqiqatlarda bu iki yanaşmanı birləşdirən hibrid metod da istifadə edilir [24].

Aşkarlanmaqdan yayınmaq üçün zərərli proqramın yaradılmasının ənənəvi praktikası metamorfik və polimorfik metodlar istifadə etməklə bir neçə obfuskasiya üsulu tətbiq etməklə mövcud zərərli proqramların yeni variantlarını yaratmaqdır [24]. Bundan əlavə, proqramın bütün binar kodu sıxlaşdırma metodları tətbiq edilməklə obfuskasiya edilir ki, onu yalnız yerinə yetirilən zaman analiz etmək mümkün olsun [24] .

SCADA serverləri və kliyentləri çox zaman köhnə, yenilənməmiş ƏS ilə təchiz olunurlar və buna görə, zərərli proqramlarla yoluxa bilərlər. Səbəblərdən biri odur ki, *SCADA* sistemləri və onların idarə etdiyi vacib istehsal əməliyyatlarını texniki xidmət üçün dayandırmaq çətindir. Beləliklə, düzəlişlər və yenilənmələr mütəmadi və ya tövsiyə olunduğu kimi yerinə yetirilmir. [25]-də əsas diqqət ənənəvi zərərli proqramların *SCADA* sistemlərinə təsirlərinə yönəldilir. Bundan başqa, məqalədə tipik *SCADA* sisteminə hücum üçün nəzərdə tutulmuş zərərli proqram nümunələrinə də baxılır və onların potensial dağıdıcı təsirləri müzakirə olunur. Bu zərərli proqramlar Modbus protokolunun boşluqlarını istifadə edirlər və şəbəkə ekranlarından və antivirus proqram təminatından yan keçmək imkanlarına malik ola bilərlər.

SİS-də zərərli proqramları aşkarlamaq üçün [26]-da qeyri-səlis test metodu təklif edilir. Təklif edilən metodda taint-analiz üçün mənbə faylı kimi SİS proqram təminatının konfiqurasiya faylı və fazzinq nümunə faylı istifadə edilir. Əvvəlcə açar verilənləri tapılır, onun dinamik taint-analizin köməyi ilə konfiqurasiya faylında potensial təhlükəsizlik təhdidi olacağı ehtimalı böyükdür. Sonra verilənlər mutasiya edilir və anomal verilənlər faylı yaradılır. Nəhayət, fazzinq testi istifadə etməklə, təhlükəsizlik təhdidlərinin əksəriyyətini aşkarlamaq olar.

Kritik tətbiqlərdə və kiber-infrastrukturda istifadə edilən sistemlərdə və xüsusilə də, inteqral sxemlərdə (İS) aşkarlanmış aparat troyanları da təhlükəsizlik problemlərini artırır. Son onillikdə meydana çıxmış aparat troyanları [27]-də tədqiq olunur və onların aşkarlanması üçün tərsinə mühəndislik əsasında və *SVM* (*ing. Support Vector Machine*) istifadə edilməklə metod təklif edilir. *SVM* təlim üçün və troyanlarla yoluxmuş İS-ləri aşkarlamaq üçün etalon qızıl İS-lərdən istifadə edir. Təklif edilmiş metodun modelləşdirmə prosesi ISCAS 85 və ISCAS 89 kimi müasir test sxemləri tətbiq edilməklə aparılmışdır və müxtəlif nüvə funksiyaları ilə *SVM*-in aşkarlama dəqiqliyini nümayiş etdirir.

Zərərli proqram təminatının aşkarlanması kritik vacib olur, çünki onlar fərdi kompüterlərdən SİS-lərə də yayılırlar. Müasir zərərli proqramlar kod morfizmi kimi qabaqcıl anti-aşkarlama mexanizmləri ilə təchiz olunmuşdur, bu da zərərli proqramların ənənəvi kod xüsusiyyətlərinə əsaslanan aşkarlama sistemlərindən yan keçməsinə imkan verir. [28]-də icra olunan binar faylları opkod (*ing. operation code*) ardıcıllığına ayırmaq və sonra *opkodları* şəkillərə çevirmək təklif edilir. Binar fayllardan yaradılmış *opkod* şəkillərini məlum zərərli proqram nümunə kodlarından yaradılmış *opkod* şəkilləri ilə müqayisə etmək üçün konvolyusiya neyron şəbəkəsindən istifadə edilir və hədəf binar exe-faylların zərərli olub-olmadığı müəyyən edilir. Nəzəri analiz və real eksperimentlərin nəticələri göstərir ki, vizual analizin köməyi ilə zərərli proqramların aşkarlanması dəqiqlik baxımından müqayisə oluna biləndir.

Məşhur *TRITON* zərərli proqram hücumu, digər sənaye kiberhücumlarından Avtomatlaşdırılmış Təhlükəsizlik Sistemi (*ing. Safety Instrumented System*) ilə birbaşa əlaqə qurması ilə fərqlənir. Sistem sənaye obyektləri üçün avtomatlaşdırılmış təhlükəsizlik sisteminin son müdafiə xəttidir, avadanlıqların sıradan çıxması və partlayış və ya yanğın kimi fəlakətli hadisələrin qarşısını almaq üçün nəzərdə tutulmuşdur. *TRITON* zərərli proqram hücumu ilə bağlı araşdırmalar [29]-da ümumiləşdirilir, ondan qorunmağa kömək edəcək iki vasitə barədə məlumat verilir. Açıqlanan araşdırmalar *TRITON* zərərli proqramı yaratmaq üçün lazım olan səylərin, bacarıqların və maliyyə qaynaqlarının o qədər də yüksək olmadığını göstərir.

Kritik infrastruktura yeni təhdidlərdən biri də girov proqram təminatı ilə hücumlardır. Girov proqramı – şəxsin və ya şirkətin vacib məlumatlarına girişi müəyyən şəkildə bloklamasına və sonra bloklamanı aradan qaldırmaq üçün müəyyən ödəmə tələb etməsinə imkan verən zərərli proqramdır. Hazırda bloklamanın ən çox yayılmış forması istifadəçinin vacib məlumatlarının şifrlənməsidir. [30]-da çoxmərhələli girov proqramı hücumları modelləşdirilir. Model *WannaCry* girov proqramı istifadə edilməklə qiymətləndirilir. Zərərli proqram hədəfə çatmaq üçün fərqli altşəbəkələrdəki zəif qovşaqları aralıq qovşaqlar kimi istifadə edir, hücum buna görə çoxmərhələli adlanır. Zərərli proqramların statik analizinin nəticələri girov proqramının müxtəlif *SCADA* və istehsal altşəbəkələrində boşluq olan qovşaqları tapmaq və sonra şəbəkədə yaymaq üçün istifadə

etdiyi metodları aşkara çıxarır. Aşkarlanmış artefaktların əsasında şəbəkənin kaskadlı seqmentasiyası təklif edilir, burada prioritet istehsal şəbəkəsi qurğularının təhlükəsizliyinə verilir.

Müəlliflər [31]-də elektrik stansiyaların fiziki məhvinə hədəflənmiş *PLC* yoluxmalarını aşkarlamaq üçün *PLC* kod analitikası sahəsində öz tədqiqatlarını müzakirə edirlər. Onların yanaşması tərsinə mühəndislik, idarəetmə nəzəriyyəsi və dinamik sistemlərin davranışına söykənir. Kodun hibrid analizində istifadə etmək üçün mürəkkəb və yüksək dinamik təhlükəsizlik xassələrini müəyyən etmək üçün təhlükəsizlik baxımından vacib kodlar tərsinə mühəndislik ilə rekonstruksiya edilir.

Ümumiyyətlə, zərərli proqram təminatının analizi sahəsində tədqiqatların əsas problemi dəqiqliyin praktiki tətbiq baxımından xeyli aşağı olmasıdır. Real praktikada istifadə olunması üçün belə alqoritmlərin dəqiqliyi 0,99-dan böyük olmalıdır. Belə dəqiqliyin əldə edilməsi siqnaturası olmayan zərərli proqramları yalnız maşın təlimi metodları əsasında aşkarlamağa imkan verərdi. Həm də, zaman keçdikcə, yeni verilənlər əldə edildikcə, bu alqoritmlərin aşkarlama dəqiqliyi artacaqdır.

SİS-lərdə kibertəhlükəsizliyin monitorinqi metodları

Monitorinq kiber-fiziki sistemlərin əsas funksiyalarından biridir – ətraf mühitin vəziyyəti, əsas fiziki və texniki parametrlərin fasiləsiz monitorinqi sistemin idarə edilməsi üçün olduqca zəruridir. Monitorinq gedişində toplanmış verilənlər analiz edilir və dəyərləndirilir, icra olunacaq gələcək əməliyyatların düzgünlüyü yoxlanır.

Monitorinq məsələsinə keçmiş müşahidələr və real zamanda daxil olan verilənlər əsasında yanaşmalar üstünlük təşkil edir. [32]-də sənaye kiber-fiziki sistemlərininn monitorinqi və idarə edilməsi sahəsində tədqiqatların müasir vəziyyəti analiz edilir və əldə olunmuş son nailiyyətlər göstərilir, həmçinin gələcək aktual tədqiqat istiqamətləri də müzakirə edilir.

Sahə cihazlarından vəziyyət qiymətlərini korrelyasiya etməklə SİS-lərdə tamlıq səhvlərinin aşkarlanması [33]-də araşdırılır. Xüsusi olaraq, klassik Bizans generalları məsələsinin SİS kontekstində bir qoyuluşu nəzərdən keçirir. Nəticələr sübut edir ki, fiziki sistemin xassələrindən istifadə edilməsi tamlıq hücumlarını aşkarlamaq üçün sistemin vəziyyətləri barədə nəticələrə gəlməyə imkan verir.

[34]-də müdaxilələrin iyerarxik paylanmış aşkarlanması vasitəsilə anomaliyaların tapılmasına, [35, 36]-də isə SİS-lərdə kiberhücumların aşkarlanmasına dərin neyron şəbəkələri yanaşmalarına baxılır. Hosic və həmmüəllifləri qərar ağaclarının evolyusiyası metodu işləmişlər [37]. Yanaşma genetik proqramlaşdırma metodlarının tətbiqinin köməyi ilə işləyir və şəbəkə anomaliyalarının axtarışına yönəlib.

Monitorinq sahəsində tədqiqatların oxşar cəhəti anomaliyaların aşkarlanmasına əsaslanmalarıdır və problemləri də oradan qaynaqlanır. Maşın təlimi üsulları anomaliyaların aşkarlanması sistemlərində normal profilin qurulması və müdaxilələrin aşkarlanmasında əsas rol oynayır [38]. Anomaliyaların aşkarlanmasında normal davranışa uyğun nişanlanmış verilənlər adətən əlyetər olur, anomal davranışa uyğun verilənlər isə mövcud olmur. Supervizorlu maşın təlimi metodlarına hücum olmayan təlim verilənləri lazımdır. Lakin real şəbəkə mühitində bu cür təlim verilənlərini əldə etmək çətindir. Bundan başqa, dəyişən şəbəkə və ya xidmətlər mühitində normal profil nümunələri də dəyişəcək. Təlim və test verilənləri arasında belə fərqlər müdaxilələrin öyrədilən aşkarlanması sistemlərində yüksək yalnış – pozitiv faizlərə gətirib çıxarır. Supervizorsuz anomaliya aşkarlanması sistemləri öyrədilən analoji sistemlərin nöqsanlarını aradan qaldıra bilər.

SİS-lərdə kiber-hücumların aşkarlanması sahəsində təklif edilən maşın təlimi modellərinin əsas problemi onların öyrədilməsi üçün kifayət qədər həcmdə verilənlərin olmamasıdır. Əlyetər verilənlər, ümumiyyətlə, informasiya təhlükəsizliyi tədqiqatları sahəsində böyük problemlərdən biridir. Çıxış yollarından biri dərin təlim metodlarından istifadə etməklə sintetik verilənlərin və ya test stendindən istifadə etməklə reallığa yaxın verilənlərin generasiyası ola bilər.

SİS-lərin kibertəhlükəsizliyi üçün honeypot yanaşmaları

Honeypot – boşluqları olan sistemlərdir, onlar bədniyyətliləri hücum etməyə təhrik etmək məqsədi ilə yaradılır [39]. Honeypot verilənləri toplamaq, hadisələri qeydə almaq, həyəcan siqnalları generasiya etmək və bədniyyətlinin sistemdə etdiyi hərəkətləri aşkarlamağa imkan verir. Honeypotlar həm təhlükəsizlik tədbiri kimi, həm də yeni əks-tədbirlərin yaradılması vasitəsi kimi istifadə edilə bilərlər.

Tədqiqatçılar rekonfiqurasiya olunan honeypot olan "buqələmun şəbəkədən" istifadə etməklə bədniyyətlilərin ələ keçirilməsinin yeni üsullarını tapırlar [39]. Honeynet (honeypotların şəbəkəsi), qabaqlayıcı tədbir kimi, SİS-lərdə erkən aşkarlama sistemi və xəbərdarlıq mexanizmi təmin edir. Honeypotlar SİS-də istənilən bədniyyətlinin aşkarlanması üçün siqnatura generasiya edir və hücumların çoxmərhələli aşkarlanmasını təmin edir. *SNAP*7 və *IMUNES* əsasında honeypotlar asanlıqla köklənir və SİS-lərdə sürətlə yerləşdirilə bilir.

Əgər honeypotlar hədəfyönümlü hücumları başladan bədniyyətliləri aldatmaq üçün qurulubsa, onlar mümkün qədər reallığa yaxın (real sistemləri imitasiya etmək baxımından) və cəlbedici olmalıdırlar. Fiziki honeypotlar real qurğulardan ibarətdirlər və reallığa ən yaxın honeypot formasıdırlar [40]. Son illər bu honeypotların SİS-lər üçün tətbiqini nümayiş etdirən bir neçə iş nəşr edilmişdir, məsələn, [40, 41].

SİS-lər ilə əlaqəli təhdidlərin mənzərəsini daha yaxşı anlamaq üçün İnternetdə aşağı qarşılıqlı əlaqə səviyyəsinə malik böyükmiqyaslı honeypot sistemi [41]-də reallaşdırılıb və 28-günlük eksperimentlərin gedişində müşahidə edilən qarşılıqlı əlaqələr analiz edilib. Müxtəlif sənaye və qeyri-sənaye protokolları üçün qarşılıqlı əlaqələrin nəticələri təsvir olunur, *SHODAN* kimi qurğuyönümlü açıq axtarış sistemində sadalanmış sənaye qurğularının təsiri də analiz edilir. Nəhayət, xarici bədniyyətli üçün nisbi cəlbediciliyini müəyyən etmək üçün bu protokolların müxtəlif kombinasiyaları müqayisə edilir.

Fiziki honeypotlar hücumları daha dərindən başa düşməyə imkan verirlər, lakin onların yaradılmasına və dəstəklənməsinə çəkilən xərclər olduqca yüksək ola bilər [42]. Bu problemi həll etmək üçün bədniyyətliləri tora salmaq üçün qurulmuş honeypotları virtuallaşdırmaq olar.

SİS üçün honeypotlar həm xərclər və xidmət asanlığı kimi ənənəvi İKT tələblərinə, həm də vaxt və determiniklik kimi konkret SİS tələblərinə cavab verməlidirlər. Bu tələbləri ödəyən realist, qənaətcil və rahat SİS honeyneti yaratmaq üçün server əsasında yüksək qarşılıqlı əlaqəli virtual SİS honeypotu qurmaq [42]-də təklif edilir. Məsələnin qoyuluşunu və tələbləri tamamlamaq üçün bədniyyətli modeli daxil edilir.

Əldə edilmiş realistlik və ya dəqiqlikdən asılı olaraq virtual honeypotları aşağı və yüksək səviyyəli qarşılıqlı əlaqəli honeypotlara bölmək olar [43]. Əvvəlki tədqiqatlarda SİS-lər üçün qarşılıqlı əlaqə səviyyəsi həm yüksək (məsələn, [41], həm də aşağı olan (məsələn, [40, 42] honeypotlar tədqiq edilmişdir.

MiniCPS platforması [44] əsasında [45]-də sutəmizləyici qurğu üçün test stendini imitasiya edən honeypot reallaşdırılmışdır. Müəlliflərin məlumatına görə, təqdim olunan reallaşdırma bir neçə cəhətdən: 1) Ethernet/IP bazasında ilk SİS honeypotu; 2) tam virtuallaşdırma texnologiyası (məsələn, virtual maşınlar şəbəkəsi) istifadə edilmədən qurulmuş yüksək interaktiv ilk SİS honeypotu; 3) *SDN* (*ing. Software-Defined Network*) kontrollerinin köməyi ilə idarə edilə bilən ilk SİS honeypotudur.

SCADA üçün honeypotlar təkcə real şəraitdə *SCADA* qurğularına yönəlmiş təhdidləri müəyyən etmək üçün deyil, həm də *SCADA* qurğuları şəbəkəsində potensial bədniyyətli hərəkətlərin erkən aşkarlanması üçün əsas alətlərdən biridir. [46]-da belə *SCADA* honeypotlardan biri – *Conpot* tədqiq olunur, onun effektiv *SCADA* emulyasiya qurğusu kimi həyat qabiliyyəti müəyyən edilir. *Conpot* honeypotunu qiymətləndirmək üçün sadə *skorinq* mexanizmi istifadə edilir. *Conpot* bədniyyətlinin etdiyi istənilən dəyişikliyi izləmək üçün qeydiyyat (*ing. logging*) sistemindən istifadə edir. Honeypot HTTP, SNMP və Modbus xidmətlərinin hadisələrini

millisaniyə dəqiqliyi ilə qeydiyyata alır və izləmə üçün mənbənin İnternet ünvanı, sorğunun tipi və sorğulanan resurslar kimi baza məlumatları təqdim edir.

SİS-ə hədəfyönümlü hücumları aşkarlamaq üçün [47]-də *CryPLH* (*Crysys PLC*) honeypot sistemi işlənir və tətbiq edilir. Bu honeypotu daha böyük təhlükəsizlik monitorinqi sisteminin hissəsi kimi reallaşdırmaq olar. *CryPLH* mövcud həlləri bir neçə aspektdə, xüsusilə də qarşılıqlı əlaqə səviyyəsində və konfiqurasiyanın asanlığı aspektində yaxşılaşdırır. Qiymətləndirmə nəticələri göstərir ki, *CryPLH* bədniyyətli baxımından bir çox cəhətdən real qurğudan fərqlənmir.

SIS-lərdə hücum davranışlarının və İnternet skanlamanın monitorinqi üçün [48]-də *DiPot* adlı paylanmış sənaye honeypot sistemi təklif edilir. *DiPot* istifadəçilərə hücumların klasterləşdirilməsi və vizuallaşdırılması xidmətləri təqdim edir və istifadəçilərə SİS təhlükəsizliyinin cari vəziyyətindən məlumatlı olmağa kömək edir. *DiPot* geniş vizuallaşdırma interfeysi ilə də təchiz edilib və istifadəçilərə yaxşı təcrübə qazandıra bilər.

SİS-lərdə təhlükəsizliyin test edilməsi üçün test stendləri

Çox zaman tədqiqatçıların real SİS-lərə giriş hüququ (imkanı) olmur. Bundan əlavə, SİS-lərin real əməliyyat mühitində kibertəhlükəsizlik üzrə tədqiqatların aparılması praktiki baxımdan məqbul deyil və buna görə, belə tədqiqatları test stendlərində aparmaq zəruridir. SİS-lərin təhlükəsizliyi üzrə test stendləri kiberhücumlardan müdafiə üzrə real və mürəkkəb eksperimentlərin aparılması və qiymətləndirilməsi üçün olduqca vacib eksperimental platformalar kimi xidmət edirlər. Bu test stendləri, ənənəvi modelləşdirmə platformalarından fərqli olaraq, kommunikasiya, idarəetmə və fiziki sistem xüsusiyyətlərini və onların qarşılıqlı asılılığını vahid mühitdə adekvat qeydə almağa imkan verir [49].

SİS test stendinin yaradılması bir çox ziddiyyətli tələblərə cavab verən mürəkkəb multidissiplinar problemdir. [50] altı ildən çox müddətdə müxtəlif tətbiqlər üçün SİS test stendlərinin tədqiqinə və yaradılmasıına əsaslanır, burada çoxsəviyyəli çevik model təklif edilir, onu SİS test stendlərinin yaradılmasını dəstəkləmək üçün istifadə etmək olar. Model istifadəçilərin geniş dairəsi üçün faydalı qaydalar təqdim edir. Bundan əlavə, o, "canlı" onlayn resursun yaradılması üçün də uzlaşdırılmış fundamental struktur təmin edir və zamanla genişləndirilə bilər.

SİS komponentlərində boşluqların və təhdidlərin çoxsəviyyəli analizi [51]-də təqdim edilir, qiymətləndirmə mühitinə real aparat komponentlərinin daxil edilməsi zəruriliyi müəyyən edilir. Bundan əlavə, *Hardware-In-The-Loop* test stendlərinin SİS kibertəhlükəsizliyinin qiymətləndirilməsində yararlı olduğu vurğulanır və digər qiymətləndirmə mühitlərindən üstünlükləri təqdim edilir.

Test stendləri ilə yanaşı, kiberpoliqonlar (*Cyber Range*) da real *SCADA* sistemlərində boşluqların və təhdidlərin aşağı xərcli analizi vasitəsi kimi xidmət edə bilər. [52]-də De Monfor Universitetində yaradılmış *CYRAN* (*CYber RANge*) təsvir olunur və onun yaradılmasına təsir etmiş kiberpoliqonların icmalı verilir. Kiberpoliqonların yaradılması zamanı qərar qəbuletmə prosesi və nəzərə alınmalı olan potensial çətinliklər detallı təsvir olunur.

Test stendlərinin, xüsusilə də real infrastruktur istifadə edilməklə qurulan stendlərin, yaradılması və dəstəklənməsi bahalıdır. Bundan əlavə, belə test stendləri, bir qayda olaraq, yalnız bir sahə üçün reprezentativ olurlar (çox zaman konkret bacarıqlar toplusuna və ya tədqiqatın fokusuna əsaslanır) və təcrid olunmaqla qurulurlar. [53]-də kritik milli infrastrukturların təhlükəsizliyi sahəsində tədqiqatlar üçün *ICS/IIoT Bristol Cyber Security Group* test stendinin layihələndirilməsi və yaradılması zamanı işlənmiş etalon arxitektura təsvir olunur.

[54]-də *SCADA* təhlükəsizliyi üzrə Avropa test stendinin lehinə fikirlər irəli sürülür. Bu stend boşluqları, təhdidləri və hücumların təsirlərini analiz etmək üçün istifadə edilə bilər və nəticədə yeni arxitekturaların dizaynına və etibarlı təhlükəsizlik həllərinə kömək edə bilər. Məqalədə ayrıca test mühitinə tələblər, tətbiq strategiyaları və potensial maneələr müzakirə olunur.

[55]-də kiber hücumların *SCADA* sisteminə təsiri öyrənilir. Bunun üçün elektrik stansiyasını imitasiya edən kiber-fiziki stend dizayn edilmişdir. Stenddə enerjinin generasiyası bloku, real

zamanlı proqramlaşdırıla bilən məntiq kontrollerləri, aktuatorlar, İMİ və idarəetmə kompüterləri vardır. Test stendi sənaye enerji müəssisəsi üçün xarakterik olan proses monitorinqi və verilənlərin toplanmasını reallaşdırır. Bu verilənlər müxtəlif hücum növlərinin aşkarlanması və kiber hücumların test stendinə mümkün təsirini göstərmək üçün bir neçə yanaşmanın tətbiqini və analizini asanlaşdırır.

Kritik SİS-lərdə kibertəhlükəsizlik problemlərinin həlli üçün bir vasitə kimi təklif olunan virtual test stendləri [56]-da təsvir olunur. Məqalədə SİS tədqiqatı üçün ədəbiyyatda təklif olunan müxtəlif növ test stendləri müzakirə olunur, müəlliflər tərəfindən hazırlanmış virtual test stendi platformasının icmalı verilir və inkişaf platforması kimi xidmət etmək üçün mövcud test stendlərini genişləndirmək məqsədilə gələcək işlərin siyahısı verilir.

Beləliklə, adekvat kibertəhlükəsizliyə malik olan sistemlərin yaradılması bir çox cəhətdən test stendlərinin mövcudluğundan asılıdır, burada cari problemləri və gələcək ideyaları qiymətləndirmək olar. Mövcud təcrübənin ümumiləşdirilməsinə, milli test stendlərinin yaradılmasına yanaşmaların icmalına, gələcək SİS test stendlərində əşyaların İnterneti, Big data, bulud hesablamaları və süni intellekt kimi qabaqcıl texnologiyaların inteqrasiya edilməsinə baxmaq lazımdır.

Nəticə

SİS-lər elektrik şəbəkəsi, neft və qaz boru kəmərləri, nəqliyyat sistemləri, su təchizatı və təmizləyici qurğuları kimi kritik infrastruktur aktivlərini monitorinq və idarə edir. Onlar səmərəliliyi, etibarlılığı və idarəolunmanı artırmaq məqsədi ilə köhnə elektromexanikiəsaslı sistemlərdən müasir informasiya və kommunikasiya texnologiyalarına əsaslanan yeni sistemlərə keçirlər. Lakin İKT-nin geniş tətbiqi bu sistemlərdə tamamilə yeni kibertəhlükəsizlik problemləri və boşluqlarının meydana çıxmasına səbəb olur. Çoxsaylı kommunikasiya kanalları, giriş və çıxış nöqtələri, texnoloji müxtəliflik və ciddi istismar tələbləri yüksək motivasiyalı düşmən üçün saysız-hesabsız imkanlar yaradır. Bu kritik aktivlərin işinə təsir edən kiberhücumlar cəmiyyət üçün dağıdıcı nəticələrə səbəb ola bilər.

Məqalədə SİS-lərdə kibertəhlükəsizliyin xüsusiyyətləri analiz edilmiş, kibertəhlükəsizlik risklərinin qiymətləndirilməsi, kibertəhlükəsizliyin monitorinqi və qiymətləndirilməsi üçün nəzərdə tutulmuş test stendləri sahəsində elmi-praktiki tədqiqatlar ətraflı təhlil olunmuş və müvafiq istiqamətlər üzrə açıq tədqiqat problemləri göstərilmişdir.

Ədəbiyyat

1. Benias N., Markopoulos A.P. A review on the readiness level and cyber-security challenges in Industry 4.0 / South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference, 2017, pp. 1–5.
2. Macaulay T., Singer B. L. Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS. Auerbach Publications, 2011, 203 p.
3. Krotofil M., Gollmann D. Industrial control systems security: What is happening? / Proc. of the 11th IEEE International Conference on Industrial Informatics, 2013, pp. 670–675.
4. Angle M.G., Madnick S., Kirtley J.L., Khan S. Identifying and anticipating cyberattacks that could cause physical damage to industrial control systems // IEEE Power and Energy Technology Systems Journal, 2019, vol. 6, no.4, pp. 172–182.
5. Xu Y., Yang Y., Li T., Ju J., Wang Q. Review on cyber vulnerabilities of communication protocols in industrial control systems / IEEE Conference on Energy Internet and Energy System Integration, 2017, pp. 1–6.
6. Morris T.H., Gao W. Industrial control system cyber attacks / Proc. of the 1st International Symposium for ICS & SCADA Cyber Security Research, 2013, pp. 22–29.
7. Bencsáth B., Pék G., Buttyán L., Felegyhazi M. The cousins of Stuxnet: Duqu, Flame, and Gauss // Future Internet, 2012, vol. 4, no.4, pp. 971–1003.

8. Karnouskos S. Stuxnet worm impact on industrial cyber-physical system security / Proc. of the 37th Annual Conference of the IEEE Industrial Electronics Society, 2011, pp. 4490-4494.
9. Hemsley K., Fisher R. A history of cyber incidents and threats involving industrial control systems / International Conference on Critical Infrastructure Protection, 2018, pp. 215–242.
10. McLaughlin S., Konstantinou C., Wang X., Davi L., Sadeghi A.R., Maniatakos M., Karri R. The cybersecurity landscape in industrial control systems // Proceedings of the IEEE, 2016, vol. 104, no.5, pp. 1039–1057.
11. Peng Y., Jiang C., Xie F., Dai Z., Xiong Q., Gao Y. Industrial control system cybersecurity research // Journal of Tsinghua University Science and Technology, 2012, vol. 52, no.10, pp. 1396–1408.
12. Bhamare D., Zolanvari M., Erbad A., Jain R., Khan K., Meskin N. Cybersecurity for industrial control systems: A survey // Computers & Security, 2020, vol. 89, Article 101677, 23 p.
13. Asghar M. R., Hu Q., Zeadally S. Cybersecurity in industrial control systems: Issues, technologies, and challenges // Computer Networks, 2019, vol. 165, Article 106946, 16 p.
14. Alladi T., Chamola V., Zeadally S. Industrial control systems: Cyberattack trends and countermeasures // Computer Communications, 2020, vol. 155, pp. 1-8.
15. Rubio J. E., Alcaraz C., Roman R., Lopez J. Current cyber-defense trends in industrial control systems // Computers & Security, 2020, vol. 87, Article 101561, 12 p.
16. Babu B., Ijyas T., Muneer P., Varghese J. Security issues in SCADA based industrial control systems / Proc. of the 2nd International Conference on Anti-Cyber Crimes, 2017, pp. 47–51.
17. Knowles W., Prince D., Hutchison D., Disso J.F.P., Jones K. A survey of cyber security management in industrial control systems // International Journal of Critical Infrastructure Protection, 2015, vol. 9, pp. 52–80.
18. Eckhart M., Brenner B., Ekelhart A., Weippl E.R. Quantitative security risk assessment for industrial control systems: Research opportunities and challenges // Journal of Internet Services and Information Security, 2019, vol. 9, no.3, pp. 52–73.
19. Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K. A review of cyber security risk assessment methods for SCADA systems // Computers & Security, 2016, vol. 56, pp. 1–27.
20. Guo Y., Lou X., Bajramovic E., Waedt K. Cybersecurity risk analysis and technical defense architecture: Research of ICS in nuclear power plant construction stage / Proc. of the 3rd IAEA International Conference on Nuclear Security: Sustaining and Strengthening Efforts, 2020, 9 p.
21. Cárdenas A.A., Amin S., Lin Z.S., Huang Y.L., Huang C.Y., Sastry S. Attacks against process control systems: risk assessment, detection, and response / Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, 2011, pp. 355–366.
22. Abdo H., Kaouk M., Flaus J.M., Masse F. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis // Computers & Security, 2018, vol. 72, pp. 175–195.
23. Stouffer K., Lightman S., Pillitteri V., Abrams M., Hahn A. Guide to industrial control systems (ics) security – NIST Special Publication (SP) 800-82 revision 2. NIST, Tech. Report, 2015, 247 p.
24. Komatwar R., Kokare M. A survey on malware detection and classification // Journal of Applied Security Research, 2020, pp. 1–31.
25. Fovino I.N., Carcano A., Masera M., Trombetta A. An experimental investigation of malware attacks on SCADA systems // International Journal of Critical Infrastructure Protection, 2009, vol. 2, no.4, pp. 139–145.
26. Peng Y., Liang J., Xu G. Malware detection method for the industrial control systems / Proc. of the 4th International Conference on Cloud Computing and Intelligence Systems, 2016, pp. 255–259.

27. Jain G., Raghuwanshi S., Vishwakarma G. Hardware trojan: Malware detection using reverse engineering and SVM / International Conference on Intelligent Systems Design and Applications, 2017, pp. 530–539.
28. Zhang J., Qin Z., Yin H., Ou L., Hu Y. IRMD: malware variant detection using opcode image recognition / IEEE 22nd International Conference on Parallel and Distributed Systems, 2016, pp. 1175–1180.
29. Di Pinto A., Dragoni Y., Carcano A. TRITON: The first ICS cyber attack on safety instrument systems / Proc. Black Hat USA, 2018, pp. 1–26.
30. Zimba A., Wang Z., Chen H. Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems // ICT Express, 2018, vol. 4, no.1, pp. 14–18.
31. Zonouz S., Rrushi J., McLaughlin S. Detecting industrial control malware using automated PLC code analytics // IEEE Security & Privacy, 2014, vol. 12, no.6, pp. 40–47.
32. Jiang Y., Yin S., Kaynak O. Data-driven monitoring and safety control of industrial cyber-physical systems: Basics and beyond // IEEE Access, 2018, vol. 6, pp. 47374-47384.
33. Arnold C., Butts J., Thirunarayan K. Detecting integrity attacks on industrial control systems / International Conference on Critical Infrastructure Protection, 2014, pp. 3–13.
34. Liu J., Zhang W., Ma T., Tang Z., Xie Y., Gui W., Niyoyita J.P. Toward security monitoring of industrial cyber-physical systems via hierarchically distributed intrusion detection // Expert Systems with Applications, 2020, 23 p.
35. Kravchik M., Shabtai A. Detecting cyber attacks in industrial control systems using convolutional neural networks / Proceedings of the Workshop on Cyber-Physical Systems Security and Privacy, 2018, pp. 72–83.
36. Huda S., Yearwood J., Hassan M. M., Almogren A. Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks // Applied Soft Computing, 2018, vol. 71, pp. 66-77.
37. Hosic J., Lamps J., Hart D H. Evolving decision trees to detect anomalies in recurrent ICS networks / World Congress on Industrial Control Systems Security, 2015, pp. 50–57.
38. Hu Y., Yang A., Li H., Sun Y., Sun L. A survey of intrusion detection on industrial control systems // International Journal of Distributed Sensor Networks, 2018, vol. 14, no.8, 14 p.
39. Dutta N., Jadav N., Dutiya N., Joshi D. Using honeypots for ICS threats evaluation / Recent Developments on Industrial Control Systems Resilience, 2020, pp. 175–196.
40. Guarnizo J.D., Tambe A., Bhunia S.S., Ochoa M., Tippenhauer N.O., Shabtai A., Elovici Y. Siphon: Towards scalable high-interaction physical honeypots / Proc. of the 3rd ACM Workshop on Cyber-Physical System Security, 2017, pp. 57–68.
41. Serbanescu A.V., Obermeier S., Yu D.Y. ICS threat analysis using a large-scale honeynet / The 3rd International Symposium for ICS & SCADA Cyber Security Research, 2015, pp. 20–30.
42. Antonioli D., Agrawal A., Tippenhauer N.O. Towards high-interaction virtual ICS honeypots-in-a-box / Proc. of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, 2016, pp. 13–22.
43. Fan W., Du Z. Fernández D. Taxonomy of honeynet solutions / SAI Intelligent Systems Conference, 2015, pp. 1002–1009.
44. Antonioli D., Tippenhauer N.O. MiniCPS: A toolkit for security research on CPS networks // Proc. of the 1st ACM Workshop on Cyber-Physical Systems Security and Privacy, 2015, pp. 91–100.
45. Abe S., Tanaka Y., Uchida Y., Horata S. Developing deception network system with traceback honeypot in ICS network // SICE Journal of Control, Measurement, and System Integration, 2018, vol. 11, no.4, pp. 372–379.
46. Jicha A., Patton M., Chen H. SCADA honeypots: An in-depth analysis of Conpot / IEEE Conference on İntelligence and Security İnformatics, 2016, pp. 196–198.

47. Buza D. I., Juhász F., Miru G., Félegyházi M., Holczer T. CryPLH: Protecting smart energy systems from targeted attacks with a PLC honeypot / International Workshop on Smart Grid Security, 2014, pp. 181–192.
48. Cao J., Li W., Li J., Li B. Dipot: A distributed industrial honeypot system / International Conference on Smart Computing and Communication, 2017, pp. 300–309.
49. Holm H., Karresand M., Vidström A., Westring E. A survey of industrial control system testbeds / Nordic Conference on Secure IT Systems, 2015, pp. 11–26.
50. Green B., Derbyshire R., Knowles W., Boorman J., Ciholas P., Prince D., Hutchison D. ICS testbed Tetris: Practical building blocks towards a cyber security resource / Proc. of the 13th USENIX Workshop on Cyber Security Experimentation and Test, 2020, pp. 1–13.
51. Keliris, A., Konstantinou, C., Tsoutsos, N. G., Baiad, R., Maniatakos, M. Enabling multi-layer cyber-security assessment of Industrial Control Systems through hardware-in-the-loop testbeds / Proc. of the 21st Asia and South Pacific Design Automation Conference, 2016, pp. 511–518.
52. Hallaq B., Nicholson A., Smith R., Maglaras L., Janicke H., Jones K. CYRAN: a hybrid cyber range for testing security on ICS/SCADA systems / Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, 2018, pp. 622–637.
53. Craggs B., Rashid A., Hankin C., Antrobus R., Serban O., Thapen N. A reference architecture for IIoT and industrial control systems testbeds / Living in the Internet of Things, 2019, 8 p.
54. Christiansson H., & Luiijf E. Creating a European SCADA security testbed / International Conference on Critical Infrastructure Protection, 2007, pp. 237–247.
55. Korkmaz E., Dolgik, A., Davi, M., Skormi, V. Industrial control systems security testbed / Proc. of the 11th Annual Symposium on Information Assurance, 2016, pp. 1–6.
56. Vaughn Jr, R.B., Morris T. Addressing critical industrial control system cyber security concerns via high fidelity simulation / Proc. of the 11th Annual Cyber and Information Security Research Conference, 2016, pp. 1–4.

УДК 004.056

Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@iit.science.az

Анализ проблем кибербезопасности в АСУ ТП

Автоматизированные системы управления технологическими процессами (АСУ ТП) широко используются для управления и мониторинга производства, снабжения электроэнергией, водоснабжения и очистки, нефтяной и нефтехимической промышленности, ядерной энергетики, транспортных систем, железных дорог и метрополитенов, они являются мозгом и основой операций в этих важнейших национальных инфраструктурах. Нарушение работы критически важной инфраструктуры может иметь быстрое и возрастающее воздействие на общество, усугубляемое высокой степенью взаимозависимости между критически важными инфраструктурами. В 2009 году вредоносное ПО Stuxnet продемонстрировало реальность и серьезность кибербезопасности АСУ ТП. В связи с широким применением концепции Индустрия 4.0 кибербезопасность АСУ ТП приобретает особую актуальность. В статье представлена краткая информация о сущности и компонентах АСУ ТП, дан краткий анализ текущего состояния их кибербезопасности. Исследования по оценке кибербезопасности АСУ ТП анализируются в областях управления рисками, методов обнаружения и анализа вредоносного программного обеспечения, технологий honeynet для мониторинга кибербезопасности и создания тестовых стендов для оценки кибербезопасности, а также для открытых исследовательских проблем в этих областях. Основные методы исследования: моделирование, сравнительные и описательные методы, методы аналогии, анализа и синтеза; основные исследовательские

подходы − систематический, комплексный и ситуативный. Ожидается, что результаты будут полезны при формировании и развитии инфраструктуры кибербезопасности промышленных систем управления в стране, совершенствовании научных исследований в области кибербезопасности SIS, а также разработке и практической реализации комплекса мер для национальной информации.
***Ключевые слова**: автоматизированные системы управления технологическими процессами, SCADA, PLC, критическая национальная инфраструктура, кибербезопасность.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@iit.science.az

Analysis of cybersecurity problems in process control systems

Industrial control systems (ICS) are widely used to control and monitor the production and supply of electricity, water supply and purification, oil and petrochemical industries, nuclear energy, transportation systems, railways and subways, they are the brain and basis of operations in these critical national infrastructures. Disruption of critical infrastructure can have a rapid and increasing impact on society, exacerbated by the high interdependence between critical infrastructures. In 2009, the Stuxnet malware demonstrated the reality and seriousness of ICS cybersecurity. In connection with the widespread use of the concept of Industry 4.0, cybersecurity of ICS is becoming especially relevant. The article provides brief information on the essence and components of the ICS, and briefly analyzes the current state of their cybersecurity. ICS cybersecurity assessment studies are analyzed in the areas of risk management, malware detection and analysis techniques, cybersecurity monitoring honeynet technologies and test benches for cybersecurity assessment, and open research issues in these areas. Basic research methods: modeling, comparative and descriptive methods, methods of analogy, analysis and synthesis; The main research approaches are systematic, complex and situational. It is expected that the results will be useful for the formation and development of cybersecurity infrastructure of industrial control systems in Azerbaijan, improvement of scientific research in the field of cybersecurity SIS, as well as for the development and practical implementation of a set of measures for national information security.
***Keywords:** Industrial control systems, SCADA, PLC, critical national infrastructure, cybersecurity.*