Neft-qaz sənayesində kibertəhlükəsizlik problemləri

Yadigar İmamverdiyev[1], Günay Muradova[2]
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

[1]yadigar@iit.science.az, [2]gmuradova9@gmail.com

***Xülasə*— Neft-qaz sənayesində istehsal tsiklinin bütün proseslərində rəqəmsal və İnternet texnologiyalarının geniş tətbiqi nəticəsində kibertəhlükəsizlik artan təhlükəyə çevrilir. Buna görə kibertəhlükəsizlik hazırda neft və qaz şirkətlərinin texnoloji inkişaf prioritetlərindən birinə çevrilir. Məqalədə neft-qaz sənayesində baş verən rəqəmsal transformasiyalara qısa xarakteristika verilir, meydana çıxan əsas kibertəhlükəsizlik təhdidləri analiz edilir və kibertəhlükəsizlik insidentləri haqqında məlumat verilir.**

Açar sözlər— neft-qaz sənayesi; rəqəmsal mədən; OT; IoT; kibertəhlükəsizlik;

I. GİRİŞ

Hazırda neft-qaz sənayesi bir sıra ciddi problemlərlə müşaiyət olunan keçid dövrünü yaşayır, bu keçid dövrü dünya bazarlarında neftin qiymətinin kəskin ucuzlaşması və xaotik dəyişkənliyi, yüngül neft ehtiyatlarının tükənməsi, ağır neft mərhələsinin genişlənməsi (həm sıxlığına, həm də çıxarılmasının çətinliyinə görə ağır neft), sahənin aparıcı oyunçuları (transmilli neft şirkətləri, neft istehsal edən ölkələr) arasında rəqabətin dərinləşməsi ilə xarakterizə edilir.

Bu keçid dövrünün əsas xarakterik cəhətlərindən biri də istehsalat tsiklinin bütün zəncirində intellektual informasiya texnologiyalarının geniş tətbiq edilməsidir. Qeyd edək ki, böyük transmilli neft-qaz şirkətləri hazırda intellektual neft-qaz yataqları texnologiyaları ilə məşğul olan xüsusi bölmələrə malikdirlər. Belə şirkətlər − Shell (“Smart Fields”), BP (“Field of the Future”), Chevron (“iFields”), həmçinin Saudi Aramco, Petrobras, Kuwait Oil və başqalarıdır. Neft-qaz şirkətləri Əşyaların İnterneti (Internet of Things, IoT), bulud texnologiyaları, Machine Learning (maşın təlimi, verilənləri emal etdikcə öyrənən alqoritmlər), yüksək məhsuldarlıqlı hesablamalar (böyük həcmli verilənlərin emalı) kimi texnologiyaların köməyi ilə neft-qaz hasilatının müxtəlif proseslərinin optimallaşdırılması metodlarının yaradılması üzərində işləyirlər [1,2]. Bu texnologiyaların tətbiqi neft-qaz yataqlarının işlənməsinin effektivliyinin yüksəldilməsinin yeni üsullarını tapmağa, neftin çıxarılması əmsalını artırmağa və xərcləri azaltmağa imkan verir.

Bununla yanaşı, rəqəmsal texnologiyaların geniş istifadəsi, kiber-strukturlardan artan asılılıq nəticəsində neft-qaz sənayesi yeni təhdidlərə məruz qalır. Neft-qaz sənayesi obyektlərinə kiberhücumlar edən bədniyyətlilərin məqsədləri müxtəlif ola bilər: kiberterrorizm, sənaye casusluğu, əməliyyatların sabotajı, verilənlərin oğurlanması və s. Neft-qaz şirkətləri kiberfəzada qarşılaşdıqları hüquqi, əməliyyat və texniki risklərin qarşısını almaq üçün müxtəlif tədbirlər görməyə məcburdurlar.

II. NEFT-QAZ SƏNAYESİ SEKTORLARININ TƏSNİFATI

Neft-qaz sənayesində xam neftin çıxarılması, emalı və məhsulların pərakəndə satışı zəncirini əhatə edən müxtəlif sektorlar vardır. Bu sektorlar ingilis dilli ədəbiyyatda uyğun olaraq, Upstream, Midstream və Downstream adlanır.

Upstream - Ümumiyyətlə, upstream təşkilatlara neft və qazın kəşfiyyatı və hasilatı daxildir. Neft və qazın kəşfiyyatı neft və qaz mədənlərinin işlənməsinə qədər axtarış, seysmik kəşfiyyat və qazma işləri daxildir. "Upsream" termini çox zaman quyu, quyuağzı, tamamlama və rezervuarı, downstream isə hasilat və emalı əhatə edir.

Midstream - neftin nəqli, emalı və saxlanması daxildir. Ona ümumi olaraq, neft qaz boru kəmərləri ilə yanaşı, qazın emalı, LNG istehsalı zavodları daxildir.

Downstream - bura neftin emalı, neft kimyası və pərakəndə satış daxildir.

III. NEFT-QAZ SƏNAYESİNDƏ ƏMƏLİYYAT TEXNOLOGİYALARI

Neft-qaz sənayesində IT texnologiyalar ilə yanaşı, sənaye avtomatlaşdırma texnologiyaları geniş istifadə edilir. Ənənəvi IT sistemlər ilə sənaye idarəetmə sistemləri arasındakı texnoloji və funksional fərqləri nümayiş etdirmək üçün “əməliyyat texnologiyaları” (ing. OT – operational technology) termini istifadə edilir. Əməliyyat texnologiyaları sistemin fiziki vəziyyətini monitorinq etmək və dəyişmək üçün istifadə edilən aparat və proqram təminatıdır.

Əməliyyat texnologiyalarına sənaye avtomatlaşdırma və nəzarət sistemlərindən SCADA (Supervisory Control And Data Acquisition), DCS (Distributed Control Systems – paylanmış idarəetmə sistemləri), PLC (Programmable Logic Controller – proqramlana bilən məntiqi sxemlər), açıq platforma kommunikasiyası serverləri, cihazlar və analizatorlar kimi mədən avadanlıqları daxildir. Əməliyyat texnologiyaları neft-qaz sektorlarında fiziki prosesləri izləmək (monitorinq) və idarə etmək üçün istifadə olunur; proseslərin parametrləri haqqında verilənlər əldə olunur və prosesləri avtomatlaşdırmaq üçün bu verilənlər istifadə edilir. Avtomatlaşdırma elektrik,

DOI: 10.25045/NCInfoSec.2018.23

mexaniki, hidravlik, pnevmatik aktuatorlar və nəzarət klapanları vasitəsilə mümkündür.

Neft-qaz dəyər zəncirində şirkətlərin tətbiq etdiyi texniki həllər Əşyaların İnterneti (Internet of Things, IoT) kimi tanınır. IoT obyektlər və maşınlar şəbəkəsi tərəfindən generasiya edilən verilənlərin toplanması, analizi və fəaliyyət göstərməyi nəzərdə tutur. Məlum olduğu kimi, IoT verilənlərə əsaslanan qərar qəbul etmək üçün lazım olan mütəmadi dəyişən verilənləri birləşdirə və analiz edə bilir. Mövcud sənaye mühitində neft-qaz şirkətləri verilənləri də karbohidrogenləri emal etdikləri kimi emal edirlər; verilənlərin generasiya edilməsi, ötürülməsi, saxlanması və emal edilməsi lazımdır. IoT strategiyalarının inkişafı ilə neft-qaz sənayesi müəssisələri “Rəqəmsal Transformasiya” əsrindən faydalanmağa çalışırlar [3].

Müasir rəqəmsal texnologiyalar dövründə informasiya tez-tez mədəndən əməliyyat texnologiyaları şəbəkəsinə, daha sonra korporativ şəbəkəyə və axırda son istifadəçiyə və əksinə, axın edə bilir. Bu eyni zamanda, troyanlar, zərərli proqramlar, girov proqramları, viruslar və s. kimi kibertəhlükələrin də varlığı deməkdir. Bədniyyətlilər İnternetdən korporativ şəbəkəyə, korporativ şəbəkədən ERP-şəbəkəyə, buradan da sənaye şəbəkəsinə keçirlər. Bu fikrin sonluğu çox kritikdir – əgər neft-qaz təşkilatlarına kiberhücumlar olsa, nəticələri çox ciddi olacaq.

Hazırda IT və OT texnologiyalarının inteqrasiyası sıxlaşır, qurğular korporativ şəbəkəyə və xarici şəbəkəyə qoşulur. İdarəetmə qurğularına asanlıqla qoşulan bədniyyətlilər daha böyük ziyan vura bilərlər. Söhbət təkcə texnoloji prosesin dayanması nəticəsində vurulan ziyandan getmir, həm də fiziki ziyan vurmaq imkanından gedir – məsələn, neft emalı və neft-kimya zavodlarında yanğın və ya partlayış törədilə bilər. Kibertəhlükəsizlik risklərinin belə miqyası onları milli səviyyəyə çıxarır [4].

IV. NEFT-QAZ SƏNAYESİNDƏ ƏSAS KİBERTƏHLÜKƏSİZLİK TƏHDİDLƏRİ

DNV GL analitika şirkəti Norveç kontinental şelfində işləyən şirkətlər üçün on ən təxirəsalınmaz kibertəhlükəsizlik təhdidlərinin siyahısını tərtib etmişdir [5]. Aydındır ki, bu təhdidləri dünyanın digər neft-qaz şirkətləri üçün də tətbiq etmək olar:

1. Kibertəhlükəsizlik sahəsində əməkdaşlar arasında məlumatlılıq və təliminin olmaması
2. Əməliyyat və təmir zamanı uzaqdan iş
3. Məlum boşluqları olan standart IT məhsulların istehsal mühitində istifadə edilməsi
4. Vendorlar, təchizatçılar və podratçılar arasında məhdud kibertəhlükəsizlik mədəniyyəti
5. Verilənlər şəbəkələrinin kifayət qədər ayrılmaması
6. Smartfonlar da daxil olmaqla, mobil cihazların və yaddaş qurğularının istifadəsi
7. Quru və dəniz qurğuları arasında verilənlər şəbəkələri
8. Verilənlər mərkəzi olan otaqların, kabinetlərin və s. yetərsiz fiziki təhlükəsizliyi olmaması
9. Həssas proqram təminatı
10. Müəssisələrdə köhnəlmiş və istifadəyə yararsız idarəetmə sistemləri

Kibertəhlükəsizlik sahəsindəki bu boşluqları risklərin qiymətləndirilməsinə əsaslanan yanaşma ilə aradan qaldırmaq olar [6]. DNV GL tərəfindən 1100 peşəkar arasında aparılmış beynəlxalq rəy sorğusu göstərmişdir ki, şirkətlər özlərinin informasiya təhlükəsizliyini fəal şəkildə idarə etsələr də, onların yalnız yarıdan bir qədər çoxu (58%) xüsusi idarəetmə strategiyası qəbul edib və yalnız 27 %-i konkret məqsədlər qoyur.

Qeyd edək ki, IT və OT fərqli missiyalar üçün yaradılıb, buna görə onların mülkiyyət sahibi və məsuliyyət də təşkilat üzrə fraqmentləşdirilib. Yeni təhdidlərin xarakteri IoT qurğular vasitəsilə hücumlar ilə əlaqəlidir. Şəbəkəyə qoşulan sensorların, ötürücülərin, smart sənaye sistemlərinin sayı sürətlə artır və hakerlər şəbəkəyə qoşulmaq üçün yeni yollar tapırlar. IoT qurğuların xüsusiyyəti ondan ibarətdir ki, onların hesablama gücü kiçikdir və onlarda müdafiə sistemləri, o cümlədən qarşılıqlı autentifikasiya və trafikin şifrlənməsi vasitələri qurmaq çətindir.

Daha bir təhdid sistemlərin qarşılıqlı asılılığının güclənməsindən, onların vahid istehsal zəncirinin həlqələrini təşkil etmələrindən qaynaqlanır. [7]-də təchizat zəncirinin hər hansı bir elementinə edilmiş kiberhücumun digər bütün qovşaqlarda öz təsirini göstərdiyi vurğulanır.

V. NEFT-QAZ SƏNAYESİNDƏ KİBERTƏHLÜKƏSİZLİK İNSİDENTLƏRİ

Neft-qaz sənayesində proqram təminatı vasitəsilə həyata keçirilən insidentlərin tarixi 1980-ci illərə gedib çıxır. ABŞ-ın yüksək rütbəli milli təhlükəsizlik rəsmisi Tomas Reed özünün “At the abyss” kitabında ABŞ-ın SSRI-yə boru kəmərinə nəzarət proqramının kodlarını Kanada şirkətindən oğurlamasına necə şərait yaratdığını qeyd etmişdir. Bu proqrama daxil edilmiş zərərli kod 1982-ci ilin iyun ayında Trans-Sibir boru kəmərində böyük bir partlayış yaratmışdı.Troyan boru kəmərində təzyiq testi keçirilən zaman işə düşmüşdü, normal təzyiqi kəskin artırmışdı və partlayışa səbəb olmuşdu [8].

2002-2003-cü ilin qışında PDVSA (Petróleos de Venezuela, S.A.) sistemlərinə kiberhücumlarda hakerlər Venesuelanın şərqindəki bir dəniz terminalında tanker yüklənməsinə məsul SCADA sisteminə nüfuz edə bilmişdilər. Hakerlar PLC-də proqramı silərək tanker yüklənməsinin qarşısını səkkiz saata almışdılar. Təcavüzkarların taktikası mükəmməl deyildi və problem nisbətən asan aşkarlanmışdı və PLC proqramları ehtiyat surətlərdən bərpa olunmuşdu.

Son 10 ildə neft-qaz sənayesində baş vermiş kibertəhlükəsizlik insidentləri haqqında aşağıda qısa xronika verilir.

2009 – Portuqaliyanın Bayamon şəhərindəki kompüterləşdirilmiş monitorinq sistemində qəfil imtina (“glitch”) baş vermişdi, bunun nəticəsində benzinlə dolu bir saxlama tankerində partlayış baş vermiş və üç gün davam edən yanğına səbəb olmuşdu.

2010 – Stuxnet virusu bütün dünyada sənaye idarəetmə sistemlərinin, o cümlədən, neftayırma zavodlarının, boru kəmərlərinin və elektrik stansiyalarının idarə edilməsi üçün istifadə edilən kompüterlərin ələ keçirilməsi istifadə edilmişdi.

2012 – dünyanın ən böyük neft istehsalçısı olan Saudi Aramco böyük bir kiberhücumun qurbanı olmuşdu. Neft nəhəngi 30 min kompüterinin virusa yoluxduğunu açıqlamışdı. Özlərini Cutting Sword adlandıran bir qrup haker Saudi Aramco hücumuna görə məsuliyyətini öz üzərinə götürdü. Onlar şirkətin sistemlərinə zərərli proqramları siyasi səbəblərə görə yoluxdurmuşdular [9].

2012 – Enerji sektorunda uzaqdan idarəetmə və monitorinq alətlərinin təchizatçısı olan Telvent şirkəti daxili şəbəkələrarası ekranın və təhlükəsizlik sistemlərinin sındırılması nəticəsində ziyan çəkmişdi. Telvent-in məlumatına görə, hər bir Fortune 100 Energy şirkəti onun sistemlərindən istifadə edir. Təcavüzkarlar köhnə IT avadanlıqlarını Smart Grid texnologiyaları ilə birləşdirməyə imkan verən məsafədən idarəetmə vasitəsi olan SCADA layihəsi ilə əlaqəli faylları oğurlamışdılar. Çox güman ki, hakerlar, enerji şirkətlərinə birbaşa hücum etmək üçün proqram təminatındakı boşluqları tapmağa çalışırdılar, buna görə mənbə kodlarını axtarırdılar.

2012 – Ugly Gorilla təxminən iyirmidən artıq ABŞ təbii qaz xidmətinə hücum edərək, qaz boru kəmərləri şirkətlərindən həssas məlumatları oğurlamışdı.

2012 – Qətərdə LNG ixrac edən aparıcı RasGas şirkətində kompüter sistemi bilinməyən virusla yoluxmuşdu, nəticədə şirkət işini bir neçə gün dayandırmışdı.

2012 – məşhur Flame zərərli proqramı Yaxın Şərqdəki şirkətdə casusluq üçün istifadə edilmişdi. Zərərli proqram səsi, ekran görüntülərini və istifadəçinin hərəkətlərini yazmaq imkanına malikdir.

2014 – Hakerlər Statoil daxil olmaqla, Norveç neft-qaz sənayesində təxminən 300 müxtəlif firmanı hədəf almışdılar. Hücum e-poçt vasitəsilə həyata keçirilmişdi. E-poçtla göndərilən məktub açıldığı zaman zərərli proqram yüklənir və təhlükəsizlikdə boşluqlar axtarılırdı.

2015 – ABŞ-da pərakəndə satış stansiyalarında benzin səviyyələrini ölçmək üçün istifadə edilən ATG (Automated Tank Gauges) cihazlarının onlayn hücum edənlər tərəfindən uzaqdan idarə edilə bilməsi aşkarlanmışdı. Təcavüzkarlar ATG-lərdə yanacaq axınını dayandıra bilərdilər.

2017 – neft-qaz şirkətləri qlobal Petya girov proqramının hücumuna məruz qalmışdı.

VI. SCADA SİSTEMLƏRİN TƏHLÜKƏSİZLİYİ ÜÇÜN STANDARTLAR

Şirkətlər SCADA sistemlərinin təhlükəsizliyini təmin etmək üçüm standartlara müraciət edirlər [6]. Amerika Milli Standartlar İnstitutu (ANSI) tərəfindən təsdiqlənmiş ISA-99.02.01 standartı belə standartlardandır (Security for Industrial Automation and Control Systems). Standart SCADA və idarəetmə sistemləri üçün kibertəhlükəsizliyin menecmenti sistemi (KMS) yaratmaq üçün yeddi əsas addım müəyyən edir.

ISA-99.02.01 addımları üç fundamental kateqoriyaya bölünüb: risk analizi, riskin KMS ilə idarə edilməsi, KMS-in monitorinqi və təkmilləşdirilməsi. Birinci kateqoriya həm cari təhlükəsizlik vəziyyətini qiymətləndirmək, həm də hansı təhlükəsizlik hədəflərinə nail olmaq istədiyini müəyyən etmək üçün mərhələlər təyin edir.

İkinci kateqoriya şirkətdə təhlükəsizlik siyasətini, təhlükəsizliyin təşkilini və təhlükəsizlik üzrə məlumatlılığı müəyyənləşdirmək üçün prosesləri əks etdirir və SCADA təhlükəsizliyinin yaxşılaşdırılması üçün təhlükəsizlik tədbirləri üzrə tövsiyələr verir. Bu kateqoriyada əsas fikir dəriniə müdafiə (ing. defense-in-depth) kimi tanınan konsepsiyadır, burada təhlükəsizlik həlləri kiberhücumların qarşısını almaq üçün diqqətlə bir neçə səviyyədə yerləşdirilir.

Son kateqoriya SCADA sisteminin yalnız KMS-ə uyğunluğunu deyil, həm də davamlı inkişaf proqramı ilə hərəkət etməsini təmin edən metodları təsvir edir.

IEC 62443 standartı sənaye avtomatlaşdırma və idarəetmə sistemləri üçün ümumi standartdır və hələ tam başa çatdırılmayıb. IEC 62443 standartlar seriyasına bütün çoxluğuna uyğunluğu təsdiqləmək çox bahalıdır və bəzi hissələr müəyyən sənaye sahələrinə aid edilməyə bilər.

Standart həmçinin təhlükəsizlik səviyyələrinə müraciət edir ki, lakin müxtəlif sistemlər üçün düzgün hədəfi müəyyən etmək çətin ola bilər. Hazırda standart nə etmək lazım olduğunu müəyyənləşdirir, lakin bunun necə ediləcəyini tam şəkildə izah etmir. Bu çətinlikləri aradan qaldırmaq üçün neft və qaz sektorunda IEC 62443 (3-2, 3-3 və 2-4) tətbiq edilməsi üçün DNV GL, Emerson, Honeywell, Shell Norveç, Siemens, Statoil və s. iştirakı ilə birgə sənaye layihəsi çərçivəsində tövsiyələr işlənmişdir. Bu layihənin məqsədi neft və qaz sektorunda sənaye avtomatlaşdırma və idarəetmə sistemlərinin təhlükəsizliyini təmin etmək üçün ümumi və praktiki yanaşma müəyyən etmək idi.

Avropa İttifaqında 2018-ci ilin may ayında qüvvəyə minən NISD (Network and Information Security Directive – Şəbəkə və İnformasiya Təhlükəsizliyi üzrə Direktiv) enerji şirkətlərinin şəbəkə və informasiya sistemlərinin minimal kiber-təhlükəsizlik standartlarına cavab verməsini təmin edir. Böyük Britaniya Milli Kibertəhlükəsizlik Mərkəzi bu Direktivə uyğunluq tələbləri üzrə ətraflı təlimat hazırlamışdır.

Direktiv “əsas xidmətlər” operatorlarını nəzərdə tutur, bu bir çox enerji şirkətini əhatə edəcək. Elektrik istehsalçıları və ötürücüləri ilə yanaşı, neft və qaz hasilatı və paylanması ilə

məşğul olan şirkətlər də bu Direktivin əhatə dairəsindədirlər. Direktiv üzv dövlətlərə "şəbəkə və informasiya sistemlərinin yüksək səviyyədə təhlükəsizliyinə nail olmaq və təmin etmək üçün müvafiq siyasət və tənzimləyici tədbirlərin" tətbiq edilməsini, habelə hadisə baş verdikdə məlumatlandırma öhdəliklərini tələb edir. Direktiv müvafiq standartların yerinə yetirilməməsinə və hadisə barədə məlumat verilməməsinə görə "effektiv, mütənasib və qərəzsiz" sanksiyalar tətbiq edilməsini tələb edir.

NƏTİCƏ

Neft-qaz sənayesi ən çox kiberhücum edilən sənaye sahələrindən biridir, bu kiberhücumların iqtisadiyyat və milli təhlükəsizlik üçün ağır potensial nəticələri ola bilər. Buna görə kibertəhlükəsizliyin təmin edilməsi neft-qaz sənayesi üçün olduqca mühüm məsələdir və kibertəhlükəsizlik tədbirləri neft-qaz əməliyyatlarının rəqəmsallaşdırılması sürəti ilə ayaqlaşmalıdır. Neft-qaz sənayesinin müxtəlif sektorları, təbii olaraq, müxtəlif risk səviyyələrinə malikdir və müxtəlif kibertəhlükəsizlik strategiyaları tələb edirlər. Mədənlərin, neft-qaz nəqlinin və emalının, ekoloji proseslərin, ümumiyyətlə, baxılan sənayedəki bütün tədbirlər kompleksinin kibertəhlükəsizlik məsələlərini həll etmək lazımdır.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikasının Dövlət Neft Şirkətinin Elm Fondunun maliyyə yardımı ilə yerinə yetirilmişdir (Layihənin adı: **“DeepOil-ML: İntellektual neft mədənləri üçün Deep Learning əsasında yeni texnologiyaların işlənməsi”**).

ƏDƏBİYYAT

[1] R.M. Alıquliyev, Y.N. İmamverdiyev, “Neft-qaz sənayesi üçün konseptual Big Data arxitekturası,” İnformasiya texnologiyaları problemləri, №1, s.3–14, 2017.

[2] R.M. Alıquliyev, Y.N. İmamverdiyev, “Neft-qaz sənayesi üçün Big Data strategiyası: Ümumi istiqamətlər,” İnformasiya texnologiyaları problemləri, №2, s. 34–47, 2017.

[3] F. Shaik, A. Abdullah, & S. Klein, Digital transformation in oil & gas - Cyber security and approach to safeguard your business. World Petroleum Congress. 2017.

[4] B. Clayton, & A. Segal, Addressing cyber threats to oil and gas suppliers. Council on Foreign Relations, 2013.

[5] Top 10 cybersecurity vulnerabilities for oil and gas // Pipeline &Gas Journal, vol. 243(2), February 2016.

[6] P. A. Ralston, J. H. Graham, & J. L. Hieb, “Cyber security risk assessment for SCADA and DCS networks,” ISA transactions, vol. 46(4), pp. 583-594, 2007

[7] M.A. Nasir, S. Sultan, S.Nefti-Meziani, & U. Manzoor, “Potential cyber-attacks against global oil supply chain,” IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1-7, 2015.

[8] E.J.Byres, “Cyber security and the pipeline control system,” Pipeline & Gas Journal, pp.58-59, 2009.

[9] C. Bronk, & E. Tikk-Ringas, ”The cyber attack on Saudi Aramco,” Survival, vol. 55(2), pp. 81-96, 2013.

CYBER SECURITY ISSUES IN THE OIL AND GAS INDUSTRY

Yadigar İmamverdiyev[1], Gunay Muradova[2]

[1,2]Institute of Information Technology of ANAS,

Baku, Azerbaijan

[1]yadigar@iit.science.az, [2]gmuradova9@gmail.com

Abstract – As a result of the widespread use of digital and Internet technologies in all the processes of the production cycle in the oil and gas industry, cyber security becomes increasing threat. Therefore, cyber security has become one of the priorities of technological development in the oil and gas companies. The article gives a brief description of the digital transformations in the oil and gas industry, analyzing the major cyber security threats and reporting on cyber security incidents.

Keywords – oil and gas industry; digital mining; OT; İoT; cyber security.