UOT 004.056

İmamverdiyev Y.N.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@lan.ab.az

İNFORMASIYA TƏHLÜKƏSİZLİYİ İNSİDENTLƏRİNİN EMALI PROSESLƏRİNİN OPTİMAL PLANLAŞDIRILMASI MODELİ

İnformasiya təhlükəsizliyi insidentlərinə tez və adekvat reaksiya verilməsi biznes-proseslərin fasiləsizliyinin təmin edilməsi üçün həlledici əhəmiyyət daşıyır. Belə insidentlərin emalı üçün xüsusi CERT-komandaların təşkil olunması tələb edilir, lakin onların saxlanması xərcləri əksər təşkilatlar üçün ağır yükdür və təşkilatlar xüsusi CERT-provayderlərin xidmətlərindən istifadə etməyə üstünlük verirlər. Bu işdə informasiya təhlükəsizliyi insidentlərinin emalı üzrə əməliyyatların operativ planlaşdırılması və CERT-qrupları arasında paylanması modeli optimallaşdırma məsələsi kimi ifadə edilmiş və onun həlli üçün diferensial evolyusiya yanaşması əsasında alqoritm işlənmişdir.

Açar sözlər: *informasiya təhlükəsizliyi, insidentin cavablandırılması, insidentlərin emalı, insidentlərin idarə edilməsi, CERT, CSIRT, optimal planlaşdırma, diferensial evolyusiya.*

Giriş

İnformasiya təhlükəsizliyinin təmin edilməsi vasitələri mükəmməl deyil, informasiya texnologiyalarında dinamik dəyişikliklər baş verir və informasiya təhlükəsizliyinin təmin edilməsinə zəruri resurslar ayırmaq mümkün olmur. Təəssüf ki, bu və digər səbəblərdən informasiya təhlükəsizliyini tam təmin etmək mümkün deyil və informasiya təhlükəsizliyinin pozulması halları – informasiya təhlükəsizliyi insidentləri baş verir. Cəmiyyətin informasiyalaşdırılması səviyyəsi artdıqca, bu insidentlər nəticəsində mümkün maliyyə itkilərinin və risklərin səviyyəsi daha da artır. Buna görə təşkilatların informasiya təhlükəsizliyi insidentlərinə tez və adekvat reaksiya verməsi vacib əhəmiyyət daşıyır. Rəqabət üstünlüyü əldə etmək üçün təkcə müdafiə olunmaq deyil, informasiya təhlükəsizliyi insidentlərinə effektiv reaksiya vermək də zəruridir. Çox zaman insidentlərin keyfiyyətli və effektiv cavablandırılmasını və idarə edilməsini təmin etməklə təşkilat insidenti zərərlə deyil, fayda ilə aradan qaldıra bilər [1].

Hələ ilk informasiya təhlükəsizliyi insidentinin emalı təcrübəsi göstərdi ki, bu işləri görmək üçün təşkilatlarda xüsusi qruplar – CERT (*ing. Computer Emergency Response Team*) komandaları təşkil edilməlidir [2]. CERT termini ABŞ-da rəsmi qeydiyyatdan keçirilmişdir və müəlliflik hüququ Karnegi-Mellon Universitetinə məxsusdur. Avropada daha çox CSIRT termini işlədilir (*ing. Computer Security and Incident Response Team, Kompüter təhlükəsizliyi və insidentləri cavablandırma qrupu*). Hazırda müxtəlif ölkələrdə çox sayda CSIRT fəaliyyət göstərir, onların müxtəlif təşkilati modelləri mövcuddur [3]. İnformasiya təhlükəsizliyi insidentlərinin sayı sürətlə artır, CSIRT-də yetərli sayda yüksəkixtisaslı mütəxəssis saxlamaq xeyli büdcə tələb edir və bunun nəticəsində bütün CSIRT-lər üçün hazırda fundamental problem artan iş yükünü məhdud insan resursları ilə balanslaşdırmaqdır [4]. Buna görə CSIRT üçün insidentlərin emalı işlərini optimal planlaşdırmaq məsələsi meydana çıxır.

Böyük miqyaslı informasiya təhlükəsizliyi insidentləri bir neçə təhlükəsizlik domenini əhatə edir. Belə insidentlər kritik infrastrukturun informasiya sistemlərinə yayıla bilər və nəticədə insanların həyatını, mülkiyyətini, iqtisadiyyatı və hətta milli təhlükəsizliyi təhdid edə bilərlər [5, 6]. Böyük miqyaslı insidentlərin sürətli identifikasiyası, informasiya mübadiləsi, təhqiqatı və koordinasiyalı şəkildə reaksiya və nəticələrin aradan qaldırılması çox zaman belə bədniyyətli hərəkətlərdən vurulan ziyanı xeyli azalda bilər. Bu insidentlərin aradan qaldırılmasına bir neçə CERT-komandası cəlb olunur ki, onların işinin koordinasiyası milli CERT-in funksiyasına daxildir. Bu zaman milli CERT işlərin optimal planlaşdırılması məsələsini həll etməli olur.

Bir çox təşkilatlar üçün informasiya təhlükəsizliyi tədbirlərini praktikada öz gücünə reallaşdırmaq mümkün olmur. Bunun səbəbləri daim dəyişən təhlükəsizlik problemlərini həll etmək üçün zəruri resursların, kadrların, ekspertlərin, texnologiyaların olmamasıdır.

İnformasiya təhlükəsizliyinin idarə edilməsi üzrə xidmətlər (*ing.Managed Security Services, MSS*) belə təşkilatların təhlükəsizlik tələblərinə cavab verə bilər. MSS provayderləri (MSSP) geniş çeşiddə təhlükəsizlik xidmətləri, o cümlədən informasiya təhlükəsizliyi insidentlərinin emalı xidmətlərini təklif edirlər. [7]-də belə xidmətlərin müxtəlif növləri, bu servisdən istifadənin fayda və riskləri müzakirə edilir, servis provayderlərinin seçilməsinə diqqətlə yanaşılmasının vacibliyi vurğulanır, belə servislərin məhsuldarlığının qiymətləndirilməsi məsələsinə də baxılır. MSSP provayderlərinin çox tələb edilən xidmətlərindən biri də informasiya təhlükəsizliyi insidentlərinin emalı üzrə xidmətlərdir.

Yuxarıda qeyd edilən səbəblərdən informasiya təhlükəsizliyi insidentlərinin real zamanda emalı üzrə işlərin CERT-qrupları arasında operativ paylanması məsələsinin həlli aktualdır. Bu işdə informasiya təhlükəsizliyi insidentlərinin emalı proseslərinin modelləşdirilməsi üçün yanaşma təklif edilir və onun həlli üçün diferensial evolyusiya (DE) alqoritmi işlənir.

İnformasiya təhlükəsizliyi insidentlərinin emalı prosesləri

İnsidentlərin emalı prosesi bir sıra ardıcıl işlərin (prosedurların) yerinə yetirilməsini tələb edir. Bu işlərin ardıcıllığı hər bir təşkilatda insidentlərin emalı qaydaları (siyasəti) ilə təsbit edilir [8]. Müxtəlif təşkilatlarda insidentlərin emalı üzrə işlərin ardıcıllığında fərqlər ola bilər. Bu həm təşkilatların özəllikləri ilə, həm də terminologiyadakı fərqlərlə əlaqədar ola bilər. Məsələ ondadır ki, "insidentlərin emalı" *(ing. incident handling*), "insidentlərin cavablandırılması" (*ing. incident response*), "insidentlərin idarə edilməsi" (*ing. incident management*) kimi terminlər çox zaman sinonim kimi işlədilir. Lakin onların arasında ciddi fərqlər vardır və insidentlərin emalı üçün tipik prosedurlar çoxluğunu müəyyən etmək üçün onlara nəzər salmaq vacibdir.

İnsidentlərin emalına insidentlərin aşkarlanması (hadisələr, insidentlər, həyəcan siqnalları haqqında məlumatların alınması və analizi), sistemləşdirmə (insidentlərə prioritetlərin verilməsi), analiz (nə baş verib, ziyan nə qədərdir, hansı təhdidə səbəb ola bilər, dəf etmək və bərpa üçün hansı addımlar lazımdır) və insidentlərin cavablandırılması (planlaşdırma, koordinasiya və həyata keçirilmə, informasiyanın yayılması, əks əlaqə və dərs çıxarma) daxildir [1].

İnsidentlərin idarə edilməsi təkcə insidentlərin emalı və insidentlərin cavablandırılmasını deyil, onların qarşısının alınmasına yönəlik fəaliyyəti də bildirir. Bu fəaliyyətə boşluqların idarə edilməsi, artefaktların idarə edilməsi, istifadəçilərin təlimi və məlumat səviyyəsinin artırılması daxildir.

ISO/IEC 27035:2011 standartı informasiya təhlükəsizliyi insidentlərinin idarə edilməsinin proses modelini təklif edir, model beş əsas mərhələdən ibarətdir [9]:

1. **Planlaşdırma və hazırlıq** – insidentlərin idarə edilməsi siyasəti işlənir və informasiya təhlükəsizliyi insidentlərinin cavablandırılması üzrə səriştəli komanda yaradılır;
2. **Aşkarlama və məlumatlandırma** – insidentlərin aşkarlanması və insident barədə məlumat verilməsi;
3. **Qiymətləndirmə və qərar qəbuletmə** – insidentlər qiymətləndirilir və insidentlərin necə emal ediləcəyi barədə qərar qəbul edilir. Məsələn, boşluğu aradan qaldırmaq və biznes-prosesləri operativ bərpa etmək olar və ya insidentin nəticələrinin aradan qaldırılması ləngisə də, kiber-cinayət barədə sübutları toplamaq olar;
4. **Cavablandırma** – ekspert analizi və insidentdən sonra bərpaetmə daxil olmaqla, insidentlərin cavablandırılması;
5. **Dərslərin çıxarılması** – informasiya təhlükəsizliyi insidentlərinin və risklərinin idarə edilməsi proseslərinin təkmilləşdirilməsi üçün dəyişikliklər.

Məqalədə baxılan məsələ üçün insidentlərin cavablandırılması prosedurlarının identifikasiya edilməsi lazımdır. İnformasiya təhlükəsizliyi insidentlərinin cavablandırılması üçün CSIRT praktikasında ən çox istifadə olunan aşağıdakı prosedurları fərqləndirmək olar [10–12]:

- **İnsidentin aşkarlanması** (və qeydiyyatı): İnsident haqqında məlumat daxil olur və ya insident hər hansı bir araşdırma vasitəsilə və ya alətlə aşkarlanır. İnsident haqqında məlumatın doğruluğu və CSIRT-in xidmət sahəsinə aid olması yoxlanılır.
- **İnsidentin sinifləndirilməsi** (*ing. triage*): İnsident sinifləndirilir, prioriteti müəyyən olunur və emal üçün bilet (ing. ticketing) açılır.
- **İnsident barəsində sübutların toplanması** və onların emalı.
- **İnsidentin lokallaşdırılması** (*ing. containment*). İnsidentin digər sistemlərə yayılmaması üçün zəruri tədbirlər həyata keçirilir.
- **İnsidentin aradan qaldırılması** (*ing. eradiction*). İstismar edilən bütün boşluqlar aşkarlanır və aradan qaldırılır. Zərəli proqram təminatı və digər arzuolunmaz komponentlər silinir.
- **İnsidentdən sonra bərpa** *(ing. recovery*). Sistem insidentdən əvvəlki vəziyyətə qaytarılır.
- **İnsident barədə hesabatın hazırlanması** *(ing. lessons learned*): baş vermiş insident analiz edilir, gələcəkdə oxşar insidentlərin qarşısını almaq üçün tövsiyələr formalaşdırılır.

İnsidentlərin cavablandırılması prosedurları insidentin növündən, onun kritiklik dərəcəsindən, mümkün zərərdən, rəhbərliyin münasibətindən və s. asılı olaraq dəyişə bilər.

Əlaqədar işlərin icmalı

İnformasiya təhlükəsizliyi insidentlərinə reaksiyanın yüksək xərcləri təşkilatları özlərinin CSİRT komandası saxlamağın məqsədəuyğunluğu barədə düşünməyə vadar edir. Eləcə də, təşkilatlar öz təhlükəsizliklərinin vəziyyəti barədə məlumatları kənar təşkilatlarla həvəssiz bölüşürlər. Onlar ümid edirlər ki, onların nüfuzuna ziyan vurmadan, ekspertlər onlara kiber-təhdidlərdən müdafiə olunmağa kömək edə bilərlər. Təşkilatların bu ehtiyaclarını qarşılamaq üçün təşkilati arxitekturada təhlükəsizlik insidentlərinə reaksiyanı dəstəkləyən koordinasiya modeli təklif edilir [13]. Bundan başqa, model real zamanda monitorinq və insident yerinin təhqiqatı zamanı rəqəmsal sübutların toplanması və səlahiyyətli orqanlara təqdim olunması funksiyasını da dəstəkləyir.

[14]-də Avstraliya maliyyə təşkilatlarında insidentlərə reaksiya praktikasında olan bir sıra əhəmiyyətli və sistematik nöqsanlar müəyyən edilir. Qeyd edilir ki, insidentə reaksiya komandaları əhəmiyyətli təcrübə toplayırlar, lakin təşkilatlar bu təcrübədən informasiya təhlükəsizliyinin idarə edilməsi proseslərini təkmilləşdirmək üçün lazımınca istifadə etmirlər. Məqalədə bu istiqamətdə bir sıra tövsiyələr və təhlükəsizlik öyrənmə modeli təklif edilir.

İnformasiya təhlükəsizliyi insidentlərinə reaksiya proseslərinin avtomatlaşdırılması çətindir və bu iş proseslərdən və texnologiyalardan kritik kömək almaqla əsasən insan tərəfindən həyata keçirilir [15]. Müasir şəraitdə insidentlərə reaksiya bir sıra səbəblərdən mürəkkəbləşir – bulud texnologiyaları və autsorsinq xidmətləri sayəsində hesablama mühitinə nəzarət itirilir, hücumların mürəkkəbliyi artır və təşkilatların təhlükəsizlik xərcləri yetərli deyil. İnformasiya təhlükəsizliyi insidentlərinə reaksiya məsələsində insanlara alternativ yoxdur, buna görə texnologiyalar bu işdə insanları dəstəkləmək, onların kritik təhlükəsizlik funksiyalarını uğurla yerinə yetirmək şansını maksimallaşdırmaq məqsədilə layihələndirilməlidir.

İlk CSIRT-lərin yaradılmasından başlayaraq onlar iş yükü, servislərin keyfiyyəti və xidmət etdikləri istifadəçilər dairəsi ilə əlaqədar xroniki problemlərlə qarşılaşdılar. Aşağı prioritetli və yüksək prioritetli insidentlərin cavablandırılması müxtəlif problemlər yaradır [4, 16]. Aşağı prioritetli insident müraciətləri eksponensial artır, bu da məhdud CSIRT resurslarını dəfələrlə üstələyir. Yüksək prioritetli insidentlərin cavablandırılmasında isə iş yükündə və xidmət keyfiyyətində uzunmüddətli qeyri-stabilliklər müşahidə edilir, xidmət etdiyi istifadəçilərdə CSIRT-in nüfuzu tədricən azalır.

Akademik baxış nöqteyi-nəzərindən baxılan məsələni məhdud resurslu planlaşdırma məsələsi kimi formalaşdırmaq olar, onu bu məqalədə insident emalının planlaşdırılması məsələsi

(*ing. Incident Response Scheduling Problem, IRSP*) adlandırırıq. IRSP məsələsini eyni anda planlaşdırma və təyinat məsələlərini həll edən məhdud resurslu layihə planlaşdırması məsələsi (*ing. Resource Constrained Project Scheduling Problem, RCPSP*) kimi də klassifikasiya etmək olar [17]. Bu məqalədə IRSP məsələsini insidentlərin emalının direktiv müddətləri çərçivəsində və minimal xərclərlə həll edilməsi üçün optimallaşdırma yanaşması təklif edilir. Məqalənin əsas töhfəsi real zamanda həll almağa imkan verən modelləşdirmə metodunun işlənməsidir. Planlaşdırma və təyinat məsələsini eyni anda həll etmək imkanı menecerlərə şərait dəyişdikcə insidentlərin emalını dəyişən şəraitə uyğun real zamanda planlaşdırmağa və həyata keçirməyə imkan verir.

RCPSP məsələsini qısaca aşağıdakı kimi ifadə etmək olar [18]. [0, T] zaman üfüqü, n sayda iş (fəaliyyət), i = 1, ..., n və r bərpa olunan resurs, k = 1, ..., r verilib. Resurs fiziki obyekt, insan, hesablama resursu (prosessor, yaddaş) ola bilər. İstənilən t = 0, ..., T zaman anında k-cı resursun sabit R_k vahidi əlyetər olur. i-ci iş p_i zaman vahidi ərzində yerinə yetirilir və bu zaman periodu ərzində k-cı resursun p_{ik} vahidi tələb edilir. Bütün verilənlərin tam ədədlər olması fərz edilir.

Məqsəd i = 1, ..., n işləri üçün $S_i \in \{0,1, \dots, T\}$ başlama vaxtlarını elə təyin etməkdir ki, resursların və işlərin üzərinə qoyulmuş məhdudiyyətlər ödənsin və məqsəd funksiyası optimal qiymət alsın. Müxtəlif məqsəd funksiyaları götürülə bilər, məsələn, $C_{max} := \max_i\{C_i\}$ yekun emal müddətinin (*ing. makespan*) minimal olması tələb edilə bilər, burada $C_i := (S_i + p_i)$ i işinin qurtarma vaxtıdır. $S = (S_i)_{i=1}^n$ vektoru layihənin planını müəyyən edir.

Qeyd edək ki, RCPSP daha ümumi modeldir, "açıq xətt" (*ing. open shop*), "iş sexi" (*ing. job shop*), "axın xətti" (*ing. flow shop*) RCPSP məsələsinin xüsusi hallarıdır. Bundan başqa, klassik kommivoyajer məsələsini, məşhur "çanta" məsələsinin müxtəlif variantlarını, konteynerlərin (xətti, ikiölçülü) qablaşdırılması məsələsini, təhsil müəssisələrində dərs cədvəllərinin tərtibi məsələsini də RCPSP məsələsi kimi ifadə etmək və həll etmək mümkündür. Bu qeydlərdən də aydındır ki, RCPSP bir çox sahədə tətbiq edilir, buna görə son dövrlər bu sahədə çox sayda məqalə nəşr edilmişdir [18]. Onun tətbiq sahələrindən istehsal proseslərinin, multiprosessorda tapşırıqların, aeroportlarda texniki xidmətin, təyyarələrə texniki baxışların, idman yarışlarının, audit heyətlərinin və s. planlaşdırılmasını göstərmək olar [19].

RCPSP kombinator optimallaşdırma məsələsidir və NP-çətin məsələlər ailəsinə daxildir [17]. Onun həlli üçün dəqiq metodlar, evristik metodlar və meta-evristik yanaşmalar olmaqla, üç əsas həll metodu var. Bu həll metodları haqqında yaxşı icmalı [20, 21]-də tapmaq olar. RCPSP məsələsinin həlli üçün genetik alqoritmin [22–24], sürü intellekti metodunun [25, 26], qarışqa sürüsü [27], arı dəstəsi metodlarının [28–30], DE alqoritminin [31, 32] müxtəlif variantları təklif edilmişdir.

Bu məqalədə qoyulmuş məsələnin həlli üçün DE alqoritmi tətbiq olunur. DE alqoritmi 1997-ci ildə R.Storn və K.Price tərəfindən təklif edilmişdir [33], klassik crossover, mutasiya və seçmə operatorlarını sadə şəkildə birləşdirən güclü evristik yanaşmadır.

Məsələnin qoyuluşu

Fərz olunur ki, CERT xidmətləri göstərən provayderə bir neçə informasiya təhlükəsizliyi insidentini emal etmək sifarişi daxil olub. İnsidentlər müxtəlif təşkilatlardan (təhlükəsizlik domenlərindən) daxil ola bilər. CERT-provayderinin əlaqələndirmə mərkəzi bu işləri özünün insidentlərin emalı üzrə ixtisaslaşmış cavablandırma qrupları (CERT-qrupları) arasında, bəzi məhdudiyyətləri nəzərə almaqla, müəyyən kriteriyalara görə optimal paylamalıdır. CERT-qrupu bir nəfərdən də ibarət ola bilər. Qeyd edək ki, hər bir insident üçün müəyyən kriteriyalar (məsələn, insidentin kritikliyi) əsasında insidentin prioriteti müəyyən edilir [34]. İnsidentin prioriteti onun nə dərəcədə operativ emal ediləcəyini və bunun üçün hansı resursların cəlb ediləcəyini təyin edir.

Aşağıdakı məhdudiyyətlər nəzərə alına bilər:

- İnsidentin emalı (cavablandırılması) bir neçə prosedurdan ibarətdir;
- Prosedurların yerinə yetirilməsi ardıcıllığı var, bəzi prosedurlara yalnız ondan əvvəl gələn bütün prosedurlar yerinə yetirildikdən sonra başlamaq olar;
- İnsidentin cavablandırılması üzrə hər bir prosedur yalnız bir cavablandırma qrupu

tərəfindən yerinə yetirilə bilər;

- Cavablandırma qrupu eyni zamanda bir neçə emal prosedurunu yerinə yetirə bilməz;
- Bir insidentin cavablandırılması üzrə bəzi prosedurları eyni anda yerinə yetirmək olar;
- Cavablandırma qrupu bir insidentin emalından digərinin emalına keçdikdə müəyyən xərclər tələb edilə bilər (bir coğrafi məkandan digərinə yerdəyişmə);
- İnsidentin emalının son müddətinə məhdudiyyət qoyula bilər (*ing. deadline*).
- Hər bir cavablandırma qrupu istənilən insident prosedurunu yerinə yetirə bilər.

Məsələnin həlli üçün optimallaşdırma modeli

Tutaq ki, J_1, J_2, …, J_n insidentlər çoxluğu R_1, R_2, …, R_m cavablandırma qrupları tərəfindən emal edilməlidir. J_i insidentinin emalı n_i prosedurdan ibarətdir (i =1, …, n). Fərz olunur ki, insidentlər bir-birindən asılı deyil və müxtəlif insidentlərin prosedurları arasında ardıcıllıq münasibətləri yoxdur. Eyni bir insidentin prosedurları isə ardıcıllıq münasibətinə görə zəncir əmələ gətirirlər: $O_{1j} \to O_{2j} \to \cdots \to O_{n_i,j}, i = 1, \dots, n$. Hər bir J_i insidenti ilə direktiv cavablandırma müddəti d_i və w_i çəkisi (kritiklik dərəcəsi və ya gecikməyə görə cərimə əmsalı) əlaqələndirilir.

Fərz olunur ki planlaşdırma üfüqü period adlanan (məsələn, saatlar) bərabər uzunluqlu zaman intervallarına bölünüb və emal müddətləri bir periodun diskret misilləridir. Prosedura başladıqdan sonra onu dayandırmaq olmaz, yəni kəsintiyə yol verilmir (*ing. preemption*). t = 0 anında bütün cavablandırma qrupları əlyetərdir və istənilən insidentin emalına başlamaq olar.

Hər bir prosedur yalnız bir cavablandırma qrupu tərəfindən emal edilə bilər. Əgər j-cu prosedur R_k cavablandırma qrupu tərəfindən yerinə yetirilirsə, onun emal müddəti t_{jk}-dır. R_k cavablandırma qrupu $[s_k^v, l_k^v], v = 1, \dots, V_k$ kəsişməyən zaman intervalları ərzində əlyetər (boş) olur, burada $l_k^v \le s_k^{v+1}, v = 1, \dots, V_k - 1$. Bundan əlavə, R_k-in toplam iş vaxtı aşağıdan H_k^- və yuxarıdan isə H_k^+ ilə məhdudlaşdırmaq olar, burada $H_k^- \le H_k^+ (k = 1, \dots, m)$.

Cədvəl 1-də illüstrasiya üçün 3 insident üçün prosedurlar siyahısı və 4 cavablandırma qrupu üçün prosedurların emal müddətləri təqdim olunur. Cədvəldən göründüyü kimi, məsələn, J_1 insidentinin cavablandırılması O_{11}, O_{12} və O_{13} prosedurlarının ardıcıl yerinə yetirilməsini tələb edir. Cədvəlin sətir və sütunlarının kəsişməsində duran ədədlər uyğun prosedurun müvafiq CERT-qrupu (R_1, R_2, R_3 və R_4) tərəfindən yerinə yetirilməsi müddətini seçilmiş zaman vahidləri ilə (məsələn, saatla) göstərir.

Cədvəl 1. Üç insident və dörd cavablandırma qrupu üçün prosedurların emal müddətləri

İnsidentlər	Prosedurlar	Prosedurların emal müddətləri			
		R_1	R_2	R_3	R_4
J_1	O_{11}	1	3	4	1
	O_{12}	3	8	2	1
	O_{13}	3	5	4	7
J_2	O_{21}	4	1	1	4
	O_{22}	2	3	9	3
	O_{23}	9	1	2	2
J_3	O_{31}	8	6	2	5
	O_{32}	4	5	8	1

Prosedurlar ardıcıllığı əsasında onların CERT-qruplarına minimal emal müddəti meyarı üzrə təyin edilməsi planı aşağıdakı kimi ola bilər:

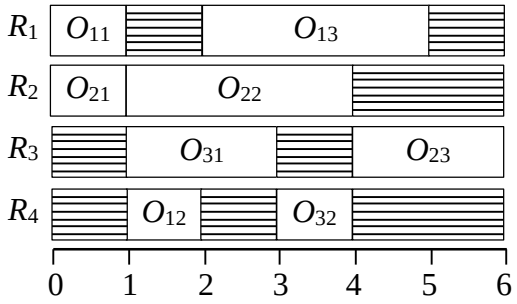
S={(O_{11}, R_1), (O_{12}, R_4), (O_{13}, R_1), (O_{21}, R_2), (O_{22}, R_2), (O_{23}, R_1), (O_{31}, R_3), (O_{32}, R_4)}

= {(O_{11}, R_1: 0-1), (O_{12}, R_4: 1-2), (O_{13}, R_1: 2-5), (O_{21}, R_2: 0-1), (O_{22}, R_2: 1-4),

(O_{23}, R_3: 4-6), (O_{31}, R_3: 1-3), (O_{32}, R_4: 3-4)}.

Plana görə, məsələn, O_{11} proseduru R_1 CERT-qrupu tərəfindən [0; 1] zaman intervalında, O_{12} proseduru R_4 CERT-qrupu tərəfindən [1; 2] zaman intervalında, O_{13} proseduru isə R_1 CERT-qrupu tərəfindən [2; 5] zaman intervalında yerinə yetirilməlidir. Beləliklə, J_1 insidentinin emalına iki CERT qrupu cəlb edilir: O_{11} və O_{13} prosedurları R_1 CERT-qrupu, O_{12} proseduru isə R_4 CERT-qrupu tərəfindən yerinə yetiriləcək.

Adətən belə tipli planları vizuallaşdırmaq üçün Qantt diaqramı istifadə edilir [18]. Yuxarıda verilmiş plana uyğun Qantt diaqramı şəkil 1-də göstərilib.



Şəkil 1. Üç insident və dörd CERT-qrupu üçün emal planının diaqramı

Diaqramdan göründüyü kimi, R_1 CERT-qrupu [1; 2] və [5; 6], R_2 CERT-qrupu [4; 6], R_3 CERT-qrupu [0; 1] və [3; 4], R_4 CERT-qrupu [0; 1], [2; 3] və [4; 6] zaman intervallarında boş olurlar.

İnsidentlərin emalının ümumi müddətini tapaq. Tutaq ki, t_{ij}^F ilə O_{ij} prosedurunun başa çatma anı işarə edilib. Yuxarıdakı plan üçün şəkil 1-dən uyğun t_{ij}^F anlarını tapmaq və onların arasından maksimumu seçməklə, ümumi emal müddətini müəyyən etmək olar. Beləliklə, insidentlərin emalının ümumi müddəti 6 zaman periodu olacaq:

$$t = max\{t_{11}^F, t_{12}^F, t_{13}^F, t_{21}^F, t_{22}^F, t_{23}^F, t_{31}^F, t_{32}^F\} = max\{1,\ 2,\ 5,\ 1,\ 4,\ 6,\ 3,\ 4\} = 6.$$

Yuxarıdakı və həmçinin yeni daxil edilmiş işarələri aşağıdakı kimi sistemləşdirək:

n – insidentlərin sayı;

m – cavablandırma qruplarının (CERT-qrupların) sayı;

n_i – i insidentində cavablandırma prosedurlarının ümumi sayı;

N – cavablandırma prosedurlarının ümumi sayı, $N = \sum_{i=1}^{n} n_i$;

O_{ij} – i insidentinin j-cu cavablandırma proseduru;

p_{ijk} – O_{ij} prosedurunun k-cı CERT-qrup tərəfindən emal müddəti;

t_{ijk} – k-cı CERT-qrupun O_{ij} prosedurunun emalına başlama vaxtı;

t_{ij}^F – O_{ij} prosedurunun başa çatma vaxtı;

i, h – insidentlərin indeksidir, i, h = 1, 2, ..., n;

k – cavablandırma qruplarının indeksidir, burada k = 1, 2, ..., m;

j, g – cavadlandırma prosedurlarının indeksidir, burada j, g = 1, 2, ..., n_i;

d_i – i-ci insidentin direktiv cavablandırma müddəti;

T_i – i-ci insidentin cavablandırılmasının gecikmə müddəti;

w_i– i-ci insidentin çəkisi (kritiklik dərəcəsi və ya gecikməyə görə cərimə əmsalı);

W_k – k-cı CERT-qrupun insidentlərin emalına sərf etdiyi ümumi müddət;

$$x_{ijk} = \begin{cases} 1, & \text{əgər } k - \text{cı cavablandırma qrupu } O_{ij} \text{ proseduruna təyin olunubsa,} \\ 0, & \text{əks halda} \end{cases}$$

Yuxarıdakı işarələrlə k-cı CERT-qrupun insidentlərin emalına sərf etdiyi ümumi W_k müddətini belə ifadə etmək olar:

$$W_k = \sum_{i=1}^{n} \sum_{j=1}^{n_j} p_{ijk} x_{ijk}, \quad (1)$$

i-ci insidentin cavablandırılmasının gecikmə müddəti T_i aşağıdakı kimi müəyyən olunur:

$$T_i = max\left(t_{i,n_i}^F - d_i, 0\right), \quad (2)$$

Adətən, insidentlərin emalını planlaşdıran zaman bir deyil, bir neçə kriteriyanı nəzərə almaq lazım gəlir. Əlbəttə, ilk növbədə insidentlərin emalına sərf olunan ümumi zaman müddətini minimallaşdırmaq lazımdır. Lakin iş yükünü CERT-qruplar arasında elə bölmək lazımdır ki, hər hansı CERT-qrup həddindən çox yüklənməsin. Eyni zamanda, kritik insidentlərin emalını da direktiv müddətlər ərzində həyata keçirmək tələb olunur. Bunu nəzərə alaraq, məqalədə insidentlərin emalı zamanı aşağıdakı kriteriyaların minimallaşdırılması məsələsi qarşıya qoyulmuşdur:

(1) İnsidentlərin emalına sərf edilən ümumi zaman müddəti;

(2) İnsidentlərin kritikliyi nəzərə alınmaqla emalın maksimum gecikmə müddəti;

(3) CERT-qrupun insidentlərin emalına sərf etdiyi ümumi müddətin maksimumu.

Yuxarıdakı işarələrdən istifadə etməklə bu kriteriyaları belə ifadə etmək olar:

$$min\, F_1 = \max_{1 \le i \le n} \left\{ \max_{1 \le j \le n_i} \left\{ t_{ij}^F \right\} \right\}, \quad (3)$$

$$\min F_2 = \max_{1 \le i \le n} \{ w_i T_i \}, \quad (4)$$

$$min\, F_3 = \max_{1 \le k \le m} \{ W_k \}. \quad (5)$$

Modeldə aşağıdakı məhdudiyyətlər vardır:

$$t_{ij}^F - t_{i,j-1}^F \ge p_{ijk} x_{ijk}, \qquad j = 2, \dots, n_i, \forall i, k \quad (6)$$

$$\left[(t_{hg}^F - t_{ij}^F - t_{hgk}) x_{hgk} x_{ijk} \ge 0 \right] \vee \left[(t_{ij}^F - t_{hg}^F - t_{ijk}) x_{hgk} x_{ijk} \ge 0 \right], \forall (i,j), (h,g), k \quad (7)$$

$$\sum_{k=1}^{m} x_{ijk} = 1, \ \ \forall i, j. \quad (8)$$

(6) şərti prosedurların ardıcıllığına olan məhdudiyyətləri təmin edir. (7) şərti hər bir CERT-qrupun ixtiyari zaman anında yalnız bir proseduru emal edə bildiyini ifadə edir. (8) şərti hər bir prosedurun emalı üçün bir cavablandırma qrupunun seçilə bildiyini göstərir.

Bu işdə çoxkriteriyalı optimallaşdırma məsələsini həll etmək üçün mövcud yanaşmalardan ən sadə yanaşma götürülmüşdür [35]. Beləliklə, ümumi məqsəd funksiyası hər birinə eyni çəki verməklə yuxarıda ifadə edilmiş məqsəd funksiyalarının çəkili cəmi kimi müəyyən edilir:

$$F = \frac{1}{3} F_1 + \frac{1}{3} F_2 + \frac{1}{3} F_3. \quad (9)$$

Optimallaşdırma məsələsi üçün həll alqoritmi

Həllin vektorlarla təsviri

Qoyulmuş optiamallaşdırma məsələsində iki altməsələ var: prosedurların CERT-qruplara təyinatı məsələsi və prosedurların ardıcıllığı məsələsi. Ona görə məsələnin həllini iki vektorla göstərmək məqsədəuyğun olardı [36]. Vektorlardan biri prosedurların permutasiyasını göstərir, digər vektor isə prosedurların CERT-qruplara təyinatını təsvir edir. Hər iki vektor N-ölçülüdür, burada N – prosedurların ümumi sayıdır. Təklif olunmuş bu təsvir metodu həllin ardıcıllıq şərtlərini ödəməsini təmin edir. Qeyd edək ki, bu iki vektoru bir vektorda birləşdirmək də olar.

Prosedurların permutasiyası vektoru. Permutasiya prosedurların ardıcıllığını ifadə etmək üçün istifadə edilir. Eyni insidentə aid olan prosedurlar vektorda eyni ədədlə işarə olunur. Prosedurların bu təsvir metodu şəkil 2-də illüstrasiya edilir.

O_{31}	O_{11}	O_{21}	O_{12}	O_{32}	O_{22}	O_{23}	O_{13}
3	1	2	1	3	2	2	1

Şəkil 2. Prosedurların permutasiyası vektoru

Məsələn, vektorun birinci elementi olan 3 ədədi insident 3-ə uyğundur, həm də insident 3-ə ilk dəfə rast gəlinir, buna görə insident 3-ün 1-ci proseduruna, yəni O_{31}-ə uyğun gəlir. Oxşar qaydada, vektorun beşinci elementi olan 3 ədədi insident 3-ün ikinci rastgəlməsidir, buna görə insident 3-ün 2-ci prosedurunu, yəni O_{32}-ni işarə edir.

CERT-qrupların təyinatı vektoru. Bu vektorun elementi uyğun prosedur üçün təyin edilmiş CERT-qrupunu işarə edir. Təyinatlar vektoru şəkil 3-də illüstrasiya edilir. Məsələn, vektorun birinci elementindən yuxarıda yazılan O_{11} onu bildirir ki, insident 1-in 1-ci proseduru CERT-qrup 1 tərəfindən yerinə yetiriləcək. Oxşar olaraq, O_{12} və O_{13} işarə edir ki, insident 1-in 2-ci proseduru CERT-qrup 4 tərəfindən, 3-cü proseduru isə yenə CERT-qrup 1 tərəfindən icra olunacaq.

O_{11}	O_{12}	O_{13}	O_{21}	O_{22}	O_{23}	O_{31}	O_{32}
1	4	1	2	2	3	3	4

Şəkil 3. CERT-qrupların təyinatı vektoru

İlkin populyasiyanın generasiyası

İlkin populyasiya alqoritmin məhsuldarlığına böyük təsir göstərir. Təklif edilən alqoritmin yaxşılaşdırılması üçün ilkin populyasiya Kacem və həmmüəlliflərinin yanaşmasından istifadə edilir [37]. Bu yanaşmada ilkin populyasiya AssignmentRule1 və AssigmentRule2 ilə generasiya olunur. AssignmentRule1 emal müddətinin minimallaşdırılmasına fokuslanır, prosedurların və CERT-qrupların ardıcıllığını müəyyən edir. AssigmentRule2 populyasiyanın müxtəlifliyini təmin edir.

İstifadə edilən alqoritmdə prosedurların və CERT-qrupların ardıcıllığı təsadüfi generasiya edilir. Təyinatlar müəyyən ediləndən sonra CERT-qruplarında prosedurların ardıcıllığı nizamlanır. Buna üç müxtəlif metodun köməyi ilə nail olurlar: təsadüfi (insident təsadüfi seçilir), əksəriyyəti qalmış iş və əksəriyyəti qalmış prosedurlar seçilir. Təklif edilmiş alqoritmdə ilkin populyasiya fərdlərinin 40 %-i AssignmentRule1, 60 %-i AssignmentRule2 istifadə edilməklə generasiya edilir, prosedurların ardıcıllığı növbə ilə yuxarıdakı üç dispetçer qaydası ilə tənzimlənir.

Diskret DE alqoritmi

DE stoxastik, populyasiya əsaslı optimallaşdırma alqoritmidir. DE alqoritminin konsepsiyası genetik alqoritmlərin də daxil olduğu geniş evolyusiya alqoritmlərindən götürülüb. Mutasiya, çarpazlaşma və seçmə kimi bir neçə mexanizm mövcud həlləri yenidən kombinasiya etməklə, yeni həllər almaq və optimal həll və ya ən azı, məsələnin şərtlərini ödəyən həllər tapmaq üçün istifadə edilir. DE kəsilməz qiymətli optimallaşdırma məsələləri üçün təklif edilmişdi [38]. [39]-də binar dəyişənlər üçün DE alqoritmi təklif edilir. DE-nin tamqiymətli optimallaşdırma məsələləri üçün variantları da təklif edilmişdir [40, 41].

Burada baxılan məsələnin həlli üçün [42]-də təklif edilmiş diskret DE (DDE) alqoritmi modifikasiya olunur. Tutaq ki, populyasiyanın fərdləri *2N*-ölçülü $x_i, \forall i \in \{1, \dots, N_p\}$ vektorları kimi təsvir edilir, burada *N* insident prosedurlarının ümumi sayıdır, N_p isə populyasiyanın həcmidir.

Mutasiya. Başlanğıcda mutasiya əməliyyatı tətbiq edilir. Mutant populyasiya üçün aşağıdakı tənlikləri istifadə etmək olar:

$$V_i^t = P_m \otimes F(x_i^{t-1}), \tag{10}$$

$$V_i^t = P_m \otimes F(x_a^{t-1}), \tag{11}$$

$$V_i^t = P_m \otimes G\left(x_g^{t-1}\right). \tag{12}$$

Burada V_i^t – t-ci iterasiyada populyasiyanın i-ci mutant fərdidir, x_i^{t-1} – $(t-1)$-ci iterasiyada populyasiyanın i-ci fərdidir; x_a^{t-1} – $(t-1)$-ci iterasiyada populyasiyadan təsadüfi seçilmiş fərddir; x_g^{t-1} – $(t-1)$-ci iterasiyada qlobal ən yaxşı həldir. G – mutasiya operatoru, P_m – mutasiya ehtimalıdır. $\otimes$ – şərt operatorudur, onun solundakı ehtimal müəyyən şərti ödədikdə, sağındakı mutasiya operatoru yerinə yetirilir.

Tutaq ki, mutant populyasiya üçün (10) tənliyi istifadə edilir. [0; 1]-dən müntəzəm paylanmış təsadüfi r ədədi seçilir. $r < P_m$ olarsa, onda t-ci iterasiyada mutant fərdi generasiya etmək üçün $V_i^t = F(x_i^{t-1})$ operatoru istifadə edilir. Əks halda, t-ci iterasiyada mutant fərd $V_i^t = x_i^{t-1}$ kimi qəbul edilir.

Krossover. Sonra sınaq fərdi adlanan fərd yaradılır, bunun üçün mutasiya edilmiş fərd (V_i^t) ilə cari populyasiyadan olan, hədəf fərd adlanan x_i^{t-1}fərdi arasında aşağıdakı qayda ilə çarpazlaşma əməliyyatı yerinə yetirilir:

$$y_i^t = P_c \otimes CR(x_i^{t-1}, V_i^t), \tag{13}$$

burada CR – krossover operatorudur, P_c – krossover ehtimalıdır. Əgər müntəzəm paylanmış $r \in (0,1)$ təsadüfi ədədi üçün $r < P_c$ olarsa, onda sınaq fərdini generasiya etmək üçün CR krossover operatoru tətbiq edilir: $y_i^t = CR(x_i^{t-1}, V_i^t)$. Əks halda sınaq fərdi $y_i^t = V_i^t$ kimi seçilir.

Seçmə. Mutasiya və çarpazlaşma proseslərindən sonra seçmə proseduru tətbiq edilir. Sınaq fərdinin uyğunluq qiyməti hesablanır və hədəf fərdin uyğunluğu ilə müqayisə edilir. Bu iki fərddən ən uyğun olanı növbəti populyasiyaya daxil edilir:

$$x_i^t = \begin{cases} y_i^t, \text{əgər } F(y_i^t) \le F(x_i^{t-1}) \\ x_i^{t-1}, \text{əks halda} \end{cases} \tag{14}$$

Populyasiyanın bütün fərdlərinə yuxarıdakı prosedurlar tətbiq edilməklə yeni populyasiya əldə edilir və bu əvvəlcədən təyin edilmiş dayanma meyarı ödənənə kimi təkrarlanır. Axırıncı nəslin ən yaxşı fərdi məsələnin həlli kimi götürülür.

Yuxarıda təklif edilmiş DDE alqoritmində mutasiya operatoru və krossover operatoru kimi genetik alqoritmlərdən götürülmüş aşağıdakı operatorlar istifadə edilir [43].

Mutasiya operatoru. Prosedurlar ardıcıllığını mutasiya etmək üçün təsadüfi prosedur seçilir, ondan bilavasitə əvvəl gələn prosedur və ondan bilavasitə sonra gələn prosedur seçilir. Tutaq ki, onların indeksləri uyğun olaraq a və b-dir. Seçilmiş prosedur (a, b) intervalında yerləşdirilir. Bu mutasiya alqoritmi ardıcıllıq məhdudiyyətini saxlayır və buna görə həllin mümkün həllər oblastından olmasını təmin edir. CERT-qrupların təyinat vektorunu mutasiya etmək üçün belə bir strategiyadan istifadə etmək təklif edilir. İş yükü maksimum olan CERT-qrupda elə prosedurlar axtarılır ki, onları yükü minimal olan CERT-qrup yerinə yetirə bilir. Belə prosedurlardan biri iş yükü minimal olan CERT-qrupa təyin edilir.

Çarpazlaşma operatoru. Həll vektorunun birinci hissəsi – prosedurlar ardıcıllığı üçün POX (*ing. precedence preserving order-based crossover*) krossover operatoru yerinə yetirilir [44], ikinci hissədə isə təsadüfi çoxnöqtəli krossover operatoru tətbiq edilir [45]. Bu yolla məhdudiyyət şərtlərini ödəyən yararlı törəmə generasiya edilə bilər.

Nəticə

Kiber-hücumların mürəkkəbliyi və neqativ nəticələri daim artır, bununla əlaqədar informasiya təhlükəsizliyi insidentlərinin sürətlə cavablandırılması biznes-proseslərin fasiləsizliyi üçün xüsusi əhəmiyyət daşıyır. Təklif edilən model emal prioritetləri nəzərə alınmaqla, insidentləri qısa müddətdə aradan qaldırmaq üçün CERT-qrupların işini optimal planlaşdırmağa imkan verir. Gələcək tədqiqatlarda müxtəlif xüsusiyyətləri nəzərə almaqla (məsələn, insidentlərin CERT-xidmətinə müxtəlif anlarda daxil olması və minimal xərclərlə aradan qaldırılması), optimallaşdırma modelinin modifikasiyaları və onun həlli üçün digər evolyusiya metodları əsasında alqoritmlərin işlənməsi nəzərdə tutulur.

Ədəbiyyat

1. Əliquliyev R.M., İmamverdiyev Y.N. İnformasiya təhlükəsizliyi insidentləri. Bakı: "İnformasiya Texnologiyaları" nəşriyyatı, 2015, 219 səh.
2. Cichonski P., Millar T., Grance T., and Scarfone K. Computer security incident handling guide. NIST Special Publication 800-61, 2012, 147 p.
3. West-Brown M.J., Stikvoort D., and Kossakowski K.-P. Handbook for Computer Security Incident Response Teams (CSIRTs). CMU/SEI-2003-HB-002. 2003, 223 p.
4. Wiik J., Gonzalez J.J., Davidsen P.I., and Kossakowski K.P. Chronic workload problems in CSIRTs / Proc. of the 27th International Conference of the System Dynamics Society, 2009, pp.1–19.
5. Osorno M., Millar T., Rager D. Coordinated cybersecurity incident handling: Roles, processes, and coordination networks for crosscutting incidents / Proc. of the 16th ICCRTS "Collective C2 in Multinational Civil-Military Operations", 2011, pp.1–12.
6. Tøndel I.A., Line M.B., Jaatun M.G. Information security incident management: Current practice as reported in the literature // Computers & Security, 2014, vol.45, pp.42–57.
7. Deshpande D. Managed security services: An emerging solution to security / Proc. 2nd Annual Conference on Information Security Curriculum Development, 2005, pp.107–111.
8. Alberts C., Dorofee A., Killcrece G., and Zajicek R. R. M. Defining incident management processes for CSIRTs: A work in progress. Carnegie Mellon Software Engineering Institute, 2004, 249 p.
9. ISO/IEC 27035:2011 Information technology – Security techniques – Information security incident management. 2011, 78 p.
10. Mitropoulos S., Patsos D., Douligeris C. On incident handling and response: A state-of-the-art approach // Computers & Security, 2006, vol.25, pp.351–370.
11. Hidayah N., Rahman A., Kim K., Choo R. A survey of information security incident handling in the cloud // Computers & Security, vol.49, 2015, pp.45–69.
12. 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.
13. Jeong K., Park J., Kim M., Noh B. A security coordination model for an inter-organizational information incidents response supporting forensic process / Fourth International Conference on Networked Computing and Advanced Information Management, 2008, vol.2, pp.143–148.
14. Atif A., Maynard S.B., and Shanks G. A case analysis of information systems and security incident responses // International Journal of Information Management, 2015, vol.35, no.6, pp.717–723.
15. Schneier B. The future of incident response // IEEE Security & Privacy, 2014, vol.12, no.5, pp.96–96.
16. Kuypers M. A., Maillart T., and Paté-Cornell E. An empirical analysis of cyber security incidents at a large organization. Working Paper. 2016, 22 p.
17. Brucker P., Drexl A., Möhring R., Neumann K., and Pesch E. Resource-constrained project scheduling: Notation, classification, models, and methods // European Journal of Operational Research, 1999, vol.112, no.1, pp.3-41.
18. Brucker P., and Knust S., Complex Scheduling. GOR-Publications, 2012, 352 p.
19. Artigues C., Demassey S., and Neron E. (Eds.) Resource-constrained project scheduling: models, algorithms, extensions and applications. John Wiley & Sons. 2008, 288 p.
20. Kolisch R., Hartmann S. Experimental investigation of heuristics for resource constrained project scheduling: an update // European Journal of Operational Research, 2006, vol.174, no.1, pp.23–37.

21. Habibi F., Barzinpour F., and Sadjadi S. Resource-constrained project scheduling problem: review of past and recent developments // Journal of Project Management, 2018, vol.3, no.2, pp.55–88.
22. Alcaraz J., Maroto C., and Ruiz R. Solving the multi-mode resource-constrained project scheduling problem with genetic algorithms // Journal of the Operational Research Society, 2003, vol.54, no.6, pp.614–626.
23. Valls V., Ballestini F., Quintanilla S. A hybrid genetic algorithm for the resource constrained project scheduling problem // European Journal of Operational Research, 2008, vol.185, no.2, pp.495–508.
24. Gen M., Gao J., and Lin L. Multistage-based genetic algorithm for flexible job-shop scheduling problem // Intelligent and Evolutionary Systems, 2009, pp.183–196.
25. Koulinas G., Kotsikas L., and Anagnostopoulos K. A particle swarm optimization based hyper-heuristic algorithm for the classic resource constrained project scheduling problem // Information Sciences, 2014, vol.277, pp.680–693.
26. Tang D., Dai M., Salido M. A., and Giret A. Energy-efficient dynamic scheduling for a flexible flow shop using an improved particle swarm optimization // Computers in Industry, 2016, vol.81, pp.82–95.
27. Myszkowski P. B., Skowroński, M. E., Olech, Ł. P., and Oślizło K. Hybrid ant colony optimization in solving multi-skill resource-constrained project scheduling problem // Soft Computing, 2015, vol.19, no.12, pp.3599–3619.
28. Li J. Q., Pan Q. K., and Gao K. Z. Pareto-based discrete artificial bee colony algorithm for multi-objective flexible job shop scheduling problems // The International Journal of Advanced Manufacturing Technology, 2011, vol.55, no.9, pp.1159–1169.
29. Akbari R., Zeighami V., and Ziarati K. Artificial bee colony for resource constrained project scheduling problem // International Journal of Industrial Engineering Computations, 2011, vol.2, no.1, pp.45–60.
30. Gao K. Z., Suganthan P. N., Pan Q. K., Chua T. J., Chong C. S., and Cai T. X. An improved artificial bee colony algorithm for flexible job-shop scheduling problem with fuzzy processing time // Expert Systems with Applications, 2016, vol.65, pp.52–67.
31. Damak J., Jarboui B., Siarry P., Loukil T. Differential evolution for solving multi-mode resource-constrained project scheduling problems // Computers & Operations Research, 2009, vol.36, no.9, pp.2653–2659.
32. Afshar-Nadjafi, B., Karimi H., Rahimi A., and Khalili S. Project scheduling with limited resources using an efficient differential evolution algorithm // Journal of King Saud University-Engineering Sciences, 2015, vol.27, no.2, pp.176–184.
33. Storn R., Price K. Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces // Journal of Global Optimization, 1997, vol.11, no.4, pp.341–354.
34. Imamverdiyev Y.N. An information security incident prioritization method / Proc. of the 7th International Conference on Application of Information and Communication Technologies, 2013, pp.183–187.
35. Hsu T., Dupas R., Jolly D., & Goncalves G. Evaluation of mutation heuristics for the solving of multiobjective flexible job shop by an evolutionary algorithm / Proc. of the IEEE International Conference on Systems, Man and Cybernetics, 2002, vol.5, pp.655–660.
36. Shao X., Liu W., Liu Q., & Zhang C. Hybrid discrete particle swarm optimization for multi-objective flexible job-shop scheduling problem // The International Journal of Advanced Manufacturing Technology, 2013, vol. 67, no.9–12, pp.2885–2901.
37. Kacem I., Hammadi S., & Borne P. Approach by localization and multiobjective evolutionary optimization for flexible job-shop scheduling problems // IEEE Transactions on Systems, Man, and Cybernetics, Part C, 2002, vol.32, no.1, pp.1–13.

38. Das S., & Suganthan P. N. Differential evolution: A survey of the state-of-the-art // IEEE Transactions on Evolutionary Computation, 2011, vol.15, no.1, pp.4–31.
39. Alguliev R. M., Aliguliyev R. M., & Hajirahimova M. S. Quadratic Boolean programming model and binary differential evolution algorithm for text summarization // Problems of Information Technology, 2012, no.2, pp.20–29.
40. Deng C., Liang C. Y., Zhao B., Yang Y., & Deng A. Y. Structure-encoding differential evolution for integer programming // Journal of Software, 2011, vol.6, no.1, pp.140–147.
41. Li H., & Zhang L. A discrete hybrid differential evolution algorithm for solving integer programming problems // Engineering Optimization, 2014, vol.46, no.9, pp.1238–1268.
42. Pan Q. K., Tasgetiren M. F., & Liang Y. C. A discrete differential evolution algorithm for the permutation flowshop scheduling problem // Computers & Industrial Engineering, 2008, vol.55, no.4, pp.795–816.
43. Pezzella F., Morganti G., Ciaschetti G. A genetic algorithm for the flexible job-shop scheduling problem // Computers & Operations Research, 2008, vol.35, no.10, pp.3202–3212.
44. Shi G. A genetic algorithm applied to a classic job-shop scheduling problem // International Journal of Systems Science, 1997, vol.28, no.1, pp.25–32.
45. Elgendy A. R., Mohammed H., & Elhakeem A. Optimizing dynamic flexible job shop scheduling problem based on genetic algorithm // International Journal of Current Engineering and Technology, 2017, vol.7, pp.368–373.

УДК 004.056

Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@lan.ab.az

Модель оптимального планирования процессов обработки инцидентов информационной безопасности

Быстрая и адекватная реакция на инциденты информационной безопасности имеет решающее значение для обеспечения непрерывности бизнес-процессов. Для обработки таких инцидентов требуются специальные команды CERT, но расходы на их содержание являются бременем для большинства организаций, и они предпочитают пользоваться услугами специальных провайдеров услуг CERT. В этом исследовании предложена модель оперативного распределения операций по обработке инцидентов информационной безопасности между группами CERT; модель сформулирована как задача оптимизации, и для ее решения разработан алгоритм дифференциальной эволюции.

Ключевые слова: *информационная безопасность, реагирование на инциденты, управление инцидентами, CERT, CSIRT, планирование, дифференциальная эволюция.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az

A model for optimal planning of information security incident response operations

A quick and adequate response to handling of information security incidents is critical for ensuring business continuity. To handle such incidents, special CERT commands are required, but the cost of maintaining them is a burden for most organizations, and they prefer to use the services of special CERT service providers. This study proposes a model for the optimal distribution of information security incident response operations between CERT groups; the model is formulated as an optimization problem, and differential evolution algorithm is developed to solve it.

Keywords: *information security, incident response, incident handling, incident management, CERT, CSIRT, scheduling, differential evolution.*