UDC 681.3.06
SCOPUS CODE 1802
https://doi.org/10.36073/1512-0996-2021-4-46-61

ტექნოლოგიური პროცესების მართვის ავტომატიზებული სისტემების უსაფრთხოება, SCADA – შეტევის ობიექტი

ჯემალ გრიგალაშვილი მართვის სისტემების დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი, საქართველო, 0160, თბილისი, მ. კოსტავას 77
E-mail: j.grigalashvili@gtu.ge

ზაურ ჯოჯუა კომპიუტერული იჟინერიის დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი, საქართველო, 0160, თბილისი, მ. კოსტავას 77
E-mail: jojuazauri@yahoo.com

ნინო ჯოჯუა კომპიუტერული იჟინერიის დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი, საქართველო, 0160, თბილისი, მ. კოსტავას 77
E-mail: jojua_nina@gmail.com

რეცენზენტები:

ქ. კოტრიკაძე, სტუ-ის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის პროფესორი
E-mail: ketino27@gmail.com

კ. ოდიშარია, სტუ-ის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის პროფესორი
E-mail: o_korneli@yahoo.com

ანოტაცია. თითქმის ყველა SCADA სისტემის პრობლემა, რაოდენ საოცრადაც უნდა მოგვეჩვენოს, არის უმნიშვნელო დაცულობა თვით საბოლოო მომხმარებლის აგდებული და მზაკვრული დამოკიდებულებისაგან.

სტატიაში განხილულია თანამედროვე ტექნოლოგიური პროცესების მართვის ავტომატიზებული სისტემები და მათ უსაფრთხოებაზე შეტევის ალბათობები. განხილულია ვირუსული ჭიაყელა Stuxnet-ი და მისი აღმოჩენა ბუშერის ატომურ ელექტროსადგურზე. გაანალიზებულია კრიტიკულად მნიშვნელოვან ობიექტებზე შეტევების განხორციელების გზები, ტექნოლოგიური პროცესების მართვის ავტომატიზებული სისტემების უსაფრთხოების ანალიზისთვის გამოყენებული ინსტრუმენტული საშუალებები. შეთავაზებულია Stuxnet ვირუსის მიერ დაზიანებული კვანძების აღმოჩენის გზები. განხილულია ტიპური ტოპოლოგიის მქონე ტექნოლო-

გიური ქსელი და მისი ტიპური საფრთხეები. გაანალიზებულია MODBUS პროტოკოლი, დისპეტჩერიზაციის სისტემა და CISCO როუტერზე დაყენებული პაროლები.

საკვანძო სიტყვები: ბუშერის ატომური ელექტროსადგური; დისპეტჩერიზაციის სისტემა; Stuxnet ვირუსი; თანამედროვე ტექნოლოგიური პროცესების მართვის ავტომატიზებული სისტემების უსაფრთხოება; SCADA; პაროლები; MODBUS პროტოკოლი; CISCO როუტერი.

შესავალი

შეიძლება ითქვას, რომ CMC ვირუსბლოკერები გაცილებით უკეთესად ართმევს თავს დაუბლოკოს მომხმარებელს ყველაფერი თავის თავის გარდა, ვიდრე ასეთივე დანიშნულების SCADA სისტემები. CMC ვირუსბლოკერების მთავარი ამოცანა, როგორც ცნობილია, არის სისტემის მუშაობის დაბლოკვა და შემდეგ დაზარალებულის იძულება გადაიხადოს მისი განბლოკვისათვის ან საკუთარ სამუშაო დოკუმენტებთან წვდომისათვის შესაბამისი ანაზღაურება.

იმისათვის, რომ ხელით დავქოლოთ ყველა სუსტი ადგილი ოპერატორის სადგურზე, საჭიროა დაახლოებით ერთსაათიანი მუშაობა პაჩების დაყენებაში, რაც განპირობებულია უსაფრთხოების პოლიტიკითა და ფაერვოლის დაყენებით. მაგრამ, ამასთანავე, არსებობს შესაძლებლობა თვითონ შევქმნათ სკრიპტი ამ ქმედებების ავტომატიზაციისათვის.

ძირითადი ნაწილი

1. ტექნოლოგიური პროცესების მართვის თანამედროვე ავტომატიზებული სისტემების (ტპმას)

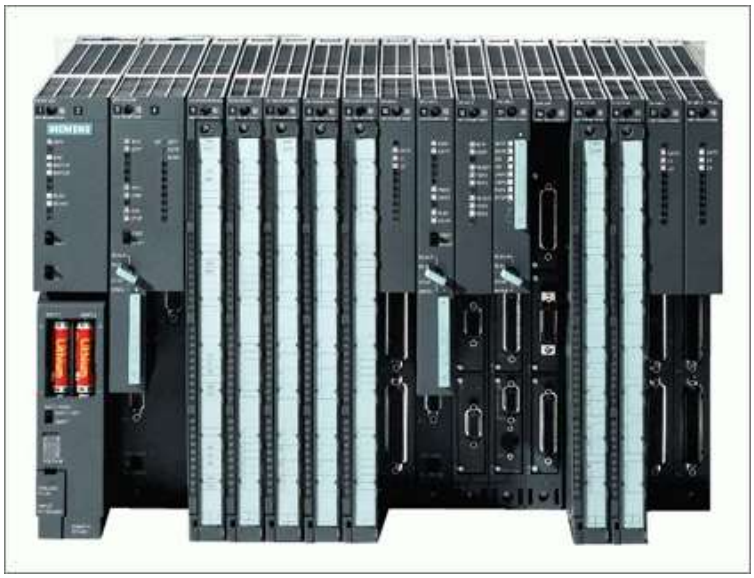
ქვემოთ მოცემული აღწერა ძირითადად ეხება ისეთი ფირმების პროდუქციას, როგორიცაა Siemens, Yokogawa, Honeywell და სხვა. ეს ტექნიკა მუშაობს საფრთხის შემცველ საწარმოებსა და დაწესებულებებში (ქიმიური, ნავთობქიმიური, ჰიდრო-, თბო- და ატომური ელექტროსადგურები და სხვ.). თავიდანვე უნდა აღინიშნოს, რომ თითოეულ ამ სისტემას სხვებთან შედარებით აქვს როგორც გარკვეული უპირატესობები, ისე ცნობილი ნაკლოვანებები. აქედან გამომდინარე, ჩვენ შევეხებით ამ სისტემების მხოლოდ საერთო მახასიათებლებს. აღნიშნული სისტემები, როგორც წესი, შედგება მართვის განაწილებული სისტემისაგან (მგს) და ავარიის საწინააღმდეგო ავტომატური დაცვის სისტემისაგან (ასადს).

ა. **მგს** არის აპარატულ-პროგრამული კომპლექსი, რომელიც თავის მხრივ შედგება შემდეგი ელემენტებისაგან:

1. საკონტროლო-გამზომი ხელსაწყოებისა და ავტომატიკისაგან (სგხ და ავტ). ეს ის აპარატურაა, რომლის მეშვეობითაც ხდება ტექნოლოგიურ პროცესზე უშუალო თვალყურის დევნება და მისი მართვა. ყოველგვარი სარქვლები, გადამკეტები, ელექტრული ჩამრაზები, წნევის, დონისა და ტემპერატურის გადამწოდები, გაზოანალიზატორები, ტუმბოები, ვაკუუმური გამწოვები და მრავალი სხვა ტიპის მოწყობილობები განეკუთვნება სგხ-სა და ავტ-ს. აღსანიშნავია, რომ ამ მოწყობილობების მიერ გენერირებული სიგნალების ტიპები შეიძლება იყოს რო-

გორც ანალოგური (4 - 20მა, 0 - 5ვ და სხვ), ისე დისკრეტული.

2. პროგრამირებადი ლოგიკური კონტროლერებისაგან (პლკ, PLC) (ფიგ. 1), რომლებიც ტპმას-ის მთავარი მმართველი ორგანოა და შედგება დუბლირებული კვების ბლოკისაგან, დუბლირებული პროცესორული მოდულებისა და დუბლირებული შემყვან-გამომყვანი მოდულებისგან. შემყვან-გამომყვან მოდულებზე უშუალოდ მიერთებულია ობიექტებთან დაკავშირებული გადამწოდები და მარეგულირებელი აპარატურა, პროცესორულ მოდულებში ჩატვირთულია ავტომატური რეგულირებისა და დამცავი ბლოკირებების მუშაობის ლოგიკა.



ფიგ. 1. პროგრამირებადი ლოგიკური კონტროლერი დუბლირებული ბლოკებით

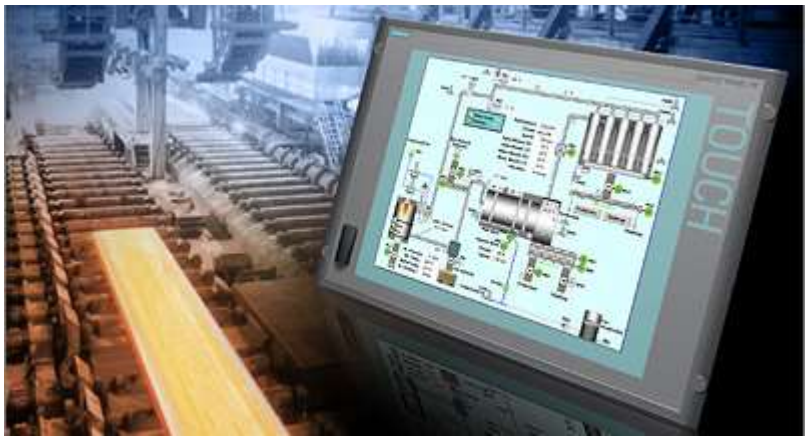
ფიგ. 2. პროგრამირებადი ლოგიკური კონტროლერი S7-1200 და S7-1500

უკანასკნელ ხანს გამოჩნდა სიმენსის ახალი ტიპის კონტროლერები, რომლებიც ფართოდ გამოიყენება დაბალი, საშუალო და მაღალი სირთულის ავტომატიზაციის სისტემების ასაგებად (ფიგ. 2). აღნიშნულმა პლკ-ებმა მთლიანად გამოდევნეს ამავე ფირმის მოძველებული S7-200 და S7-300 მოდელები მართვის თანამედროვე ავტომატიზებულ სისტემებში გამოყენებისაგან.

უნდა აღინიშნოს, რომ S7-1200 და S7-1500 პლკები სტუ-მა შეიძინა რუსთაველის ეროვნული სამეცნიერო ფონდის გრანტის დაფინანსებით განლაგებულია სტუ-ის მართვის სისტემების დეპარტამენტში და გამოიყენება სწავლების პროცესში.

3. ადამიანი-მანქანის ინტერფეისისაგან (ფიგ. 3), რომელიც ჩვეულებრივ წარმოადგენს პერსონალურ კომპიუტერს მასზე დაყენებული ОС Windows და სპეციფიკური პროგრამული უზრუნველყოფით, რომლის დახმარებითაც სრულდება ტპმას-ის კონფიგურირება. ასეთ კომპიუტერებს, ჩვეულებრივ, ყოფენ რამდენიმე ტიპად: ოპერატორის სადგური, ინჟინრის სადგური, საკონტროლო-საზომი ხელსაწყოების საინჟინრო სადგური.

სისტემასთან წვდომის უფლების ხარისხი ოპერატორებისათვის შეიძლება იყოს სხვადასხვა. ჩვეულებრივ რიგით ოპერატორებს არა აქვთ წვდომა იმ აპარატურასთან, რომლის მუშაობაც მოქმედებს უსაფრთხოებაზე, ყველაზე დიდი უფლებები (თუმცა ინჟინერზე ნაკლები) აქვს ცვლის უფროსს. ამასთანავე, გასათვალისწინებელია, რომ ოპერატორის სადგურიდან პლკ-ს დაპროგრამება შეუძლებელია. **სგხ** და **ავტ**-ის ინჟინრის სადგურს აქვს უფრო მეტად გამოყენებითი შესაძლებლობები, უზრუნველყოფენ საველე აპარატურის კონტროლს და დიაგნოსტიკას.



ფიგ. 3. ადამიანი-მანქანის ინტერფეისის ეკრანი

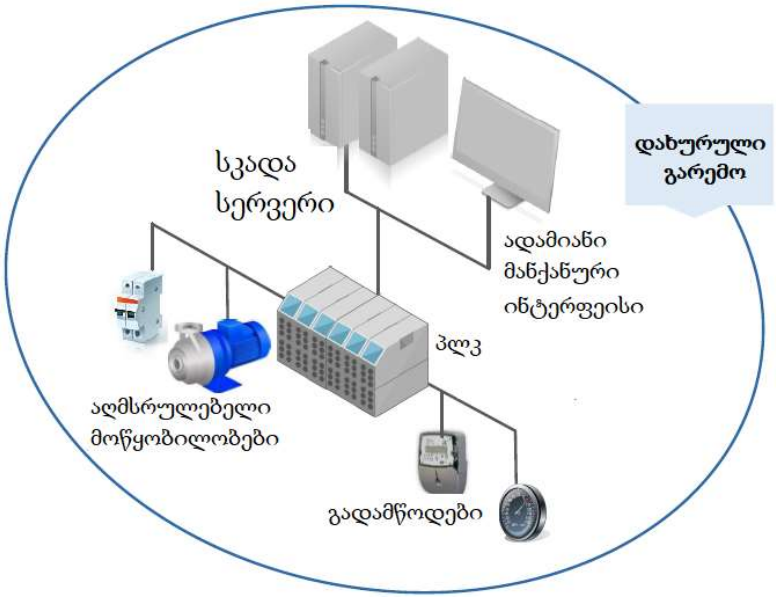
ბ. **ასადს** - ავარიის საწინააღმდეგო ავტომატური დაცვის სისტემის ძირითადი ამოცანაა წარმოების გადაყვანა უსაფრთხო ფუნქციონირების რეჟიმში **მგს**-ს მუშაობისას წარმოქმნილი რაიმე პრობლემის შემთხვევაში და დარეზერვებული აპარატურის მართვაზე გადასვლა.

ეს პრობლემებია ტექნოლოგიური პროცესების გამოსვლა დასაშვები ზღვრებიდან, აპარატურის

მტყუნება, არასაშტატო სიტუაციები და სხვ. როგორც წესი, ასეთი სისტემა მონაცემებს იღებს დუბლირებული გადამწოდებიდან (ერთ-ერთ ყველაზე საიმედო სქემად ითვლება „2OO3“, როდესაც ამუშავდება 2 ნებისმიერი გადამწოდი ერთ წერტილში დაყენებული სამი გადამწოდიდან. ეს ფაქტი ითვლება აუცილებელ პირობად დამცავი ბლოკირების ამუშავებისათვის). **ასადს**-ის სისტემას არა აქვს ოპერატორის სადგური, აქვს მხოლოდ საინჟინრო სადგური, რითაც ხდება სისტემის **პლკ**-ს კონფიგურირება. **მგს**-ს ოპერატორის სადგურიდან შეიძლება ვნახოთ, თუ როგორ მუშაობს ავარიის საწინააღმდეგო დაცვის სისტემა, მაგრამ მისი მართვა არ შეუძლია.

თანამედროვე კლასიკურ **ტპმას**-ს ახასიათებს შემდეგი თავისებურებები (ფიგ. 4):

- ოპერატორის ზოგიერთი სადგურის მწყობრიდან გამოსვლის შემთხვევაში ტექნოლოგიური პროცესის ავტომატური მართვა გრძელდება. თუ საჭირო გახდება, უნდა დაემატოს პირობები, რომლის წარმოქმნისას ყველა სადგურის მტყუნებამ უნდა გამოიწვიოს წარმოების უსაფრთხო გაჩერება;
- ოპერატორის სადგურები მიერთებულია წარმოების ქსელს, მაგრამ ჩვეულებრივად არა აქვს დაშვება ინტერნეტის ქსელთან, არა აქვს USB დამგროვებლების მიერთების შესაძლებლობა და არა აქვს დისკიდან წამკითხავი საშუალებები. ასევე, ხშირად ოპერატორის სადგურებს არა აქვს სტანდარტული კომპიუტერული კლავიატურები და აღჭურვილი არიან სპეციალიზებული კლავიატურით, რომლებსაც აქვს მხოლოდ აუცილებელი ფუნქციური ღილაკები;
- საინჟინრო სადგურები, ჩვეულებრივ, გამორთულია ან ძილის რეჟიმშია.

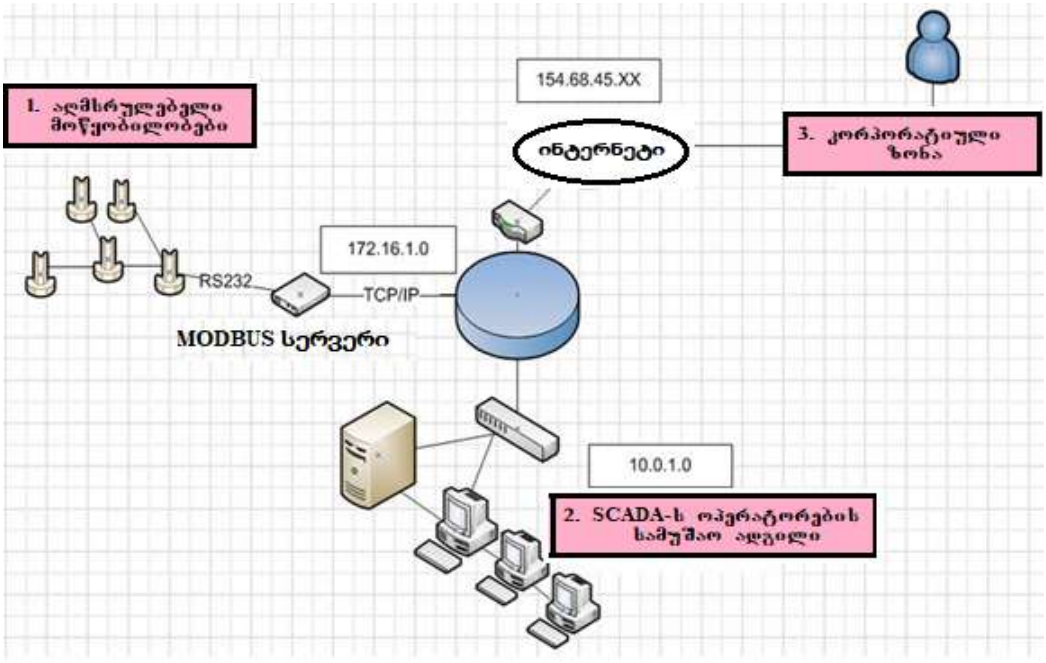


ფიგ. 4. კლასიკური ტექნოლოგიური პროცესების მართვის ავტომატიზებული სისტემა

2. ტპმას-ის ტიპური დაუცველობები

განვიხილოთ ცხადად, თუ რა სახის ხიფათს შეიცავს ტექნოლოგიური ქსელის ტიპური ტოპოლოგია (ფიგ. 5).

ტიპურ ტოპოლოგიაში, ტექნოლოგიური პროცესის ბუნებიდან გამომდინარე, ცალკე გამოყოფენ სამ ზონას – კორპორატიულს (რომელსაც არ აქვს კავშირი მართვასთან და დაკავებულია მხოლოდ ბიზნეს-პროცესებით); აღმასრულებელს (უშუალო რგოლი, სადაც სრულდება ტექნოლოგიური პროცესი, მაგალითად, ამიაკის გადამუშავება ან, მაგალითად, ნავთობის მოძრაობის მართვა და სხვ.) და დისპეტჩერიზაციისას (ეს ის ზონაა, სადაც მუშაობენ **ტპმას**-ის ოპერატორები ანუ ის თანამშრომლები, რომლებმაც შეიძლება გავლენა მოახდინონ ტექნოლოგიური პროცესების მიმდინარეობაზე).



ფიგ. 5. ტექნოლოგიური ქსელის ტიპური ტოპოლოგია

აღმსრულებელ მოწყობილობებსა და ტელემეტრიულ ქვესისტემაში შეიძლება დაგროვდეს შეტყობინებები იმ განგაშისა და ავარიული სიტუაციების შესახებ, რაც საკმაოდ კრიტიკულია მოცემული მომენტისათვის. ამასთან დაკავშირებით, ძალზე მნიშვნელოვანია აღნიშნულ ბლოკებს მიეკუთვნოს საყოველთაოდ დასაშვები IP-მისამართები, რაც სამწუხაროდ ძალიან ხშირად გვხვდება. ზოგიერთ სიტუაციაში ამ პრობლემიდან თავის არიდება შეუძლებელია ქსელის დაპროექტების პროცესში. მაგალითად, თანამედროვე სამრეწველო კონტროლერები შეიძლება შეერთებული იყოს პირდაპირ ან მოდემის გავლით. მოდემის გავლით შეერთებისას მათ, ჩვეულებრივ, აერთებენ GPRS/GSM მოდემებით, რაც ავტომატურად იწვევს მობილურ ოპერატორზე IP- მისამართის მინიჭებას. ასეთი კონფიგურაციის შემთხვევაში ისინი ძალიან დაუცველნი ხდებიან გარე შეტევებისგან. სპეციალიზებული უტილიტებითა და

მეთოდებით ბოროტგანმზრახველმა შეიძლება აღმოაჩინოს ასეთი მოწყობილობები და დააზიანოს ისინი. თვითონ აღმსრულებელი მოწყობილობები მიერთებულია MODBUS სერვერთან მიმდევრობით (RS-232/RS-485) ინტერფეისის გავლით, ხოლო ეს უკანასკნელები იმართება ოპერატორებით ხდება TCP/IP პროტოკოლის გამოყენებით Ethernet / Industrial Ethernet არხის გავლით.

დაუცველობის (საფრთხეების) სრული სურათის შესაქმნელად გთავაზობთ არაერთ მონაცემს და მათ ანალიზს სპეციალიზებული წყაროებიდან (ჩვენს შემთხვევაში ძირითადად გამოყენებულია კომპანია Positive Technologies მასალები). მონაცემთა ნაწილი აღებულია სხვა წყაროებიდანაც, როგორიცაა: დაუცველობის (საფრთხეების) ცოდნის ბაზა (vulnerability databases), საექსპლუატაციო პაკეტები (packs), მწარმოებლების შეტყობინებები, სამეცნიერო კონფერენციების და სპეციალიზებული საიტების მასალები. დაუცველობის კვლევას ტპმას-ის სფეროში დასაბამი მისცა Stuxnet ჭიის აღმოჩენამ ირანის ატომურ ელექტროსადგურ ბუშერში. ქვემოთ მოცემულია მასალები 2005-2018 წლებში აღმოჩენილი საფრთხეების შესახებ **ტპმას**-ში (იხ. ცხრ. 1) და განმარტებულია მათი ზოგადი პარამეტრები.

როგორც ცხრილიდან ჩანს, 2010-2012 წლებში აღმოჩენილი საფრთხეების რაოდენობა თითქმის 20-ჯერ აღემატება მანამდე აღმოჩენილებს. ამ საფრთხეებიდან ყველაზე მეტი აღმოაჩნდა ავტორიტეტულ კომპანიებს, Siemens-42-ს, Schneider Electric-30-ს, Advantech/Broadwin-22-ს და General Electric-15-ს. ეს განაპირობა ამ კომპანიების პროდუქციის ფართო გამოყენებამ. ბევრმა მათგანმა თვითონ დაიწყო საფრთხეების ძებნა და აღმოფხვრა. მაგალითად, Siemens-მა შექმნა სპეციალური ქვედანაყოფი Siemens ProductCERT. Computer Emergency Response Team (CERT) – კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი – http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm.

ცხრილი 1

წლები	დაუცველობის (საფრთხეების) რაოდენობა
2005	1
2007	3
2010	11
2011	64
2012	98
2013	158
2014	181
2012	212
2016	115
2017	197
2018	257
2019	გამოქვეყნდება 2022 წელს

ამ დაუცველობის 65% განეკუთვნება მაღალი და საშუალო დონის რისკებს. რისკები ფასდება 10-ბალიანი სკალით და განაწილებულია შემდეგი წესით (იხ. ცხრილი 2):

ცხრილი 2

$0,0 < CVSS \le 3,9$ – დაბალი დონის რისკი;

$4,0 \le CVSS \le 6,9$ – საშუალო დონის რისკი;

$7,0 \le CVSS \le 10,0$ – მაღალი დონის რისკი.

სადაც, CVSS - Common Vulnerability Scoring System – არის დაუცველობის შეფასების საერთო სისტემა.

2018 წელს კვლავ გრძელდებოდა შეტევები **ტპმას**-ის მიმართულებით. ამ მიზნით გამოიყენეს Stuxnet-ის ტიპის კიბერიარაღი Triton და Industroyer, რომლებიც გამიზნული იყო **ტპმას**-ის აპარატურაზე თავდასხმისათვის. მოხდა კიბერშეტევები Boeing - ის და Taiwan Semiconductor Manufacturing Company - ის სამრეწველო კომპანიების ობიექტებზე. მართალია, შეტევა განხორციელდა IP - ინფრასტრუქტურაზე, მაგრამ უარყოფითი შედეგი მაინც გამოიწვია ტექნოლოგიური პროცესების მართვაში (ტაივანში ქარხნის გაჩერება). IP - ინფრასტრუქტურებში შეღწევა გზას ხსნის ტექნოლოგიურ ქსელში შეღწევისათვის. კვლევებმა აჩვენა, რომ სამრეწველო ორგანიზაციების 82% მზად არ არის წინ აღუდგეს შიგა თავდამსხმელებს, რომელებიც ცდილობენ კორპორატიული ქსელიდან შეაღწიონ ტექნოლოგიურში. ამ ქმედების გავრცელებული სახეა ცნობილი დაუცველობების გამოყენება. საერთოდ, 2018 წელს გამოვლინდა 257 დაუცველობა, რომელთაგან 243 გამოკვლეულია და შედეგები – გამოქვეყნებული, ხოლო 14 შესწავლის პროცესში იყო. საფრთხეების განაწილება მწარმოებლებზე ასეთია: Schneider Electric - 69, Siemens - 66, Advantech - 37, Moxa - 36 და ა.შ. მოწყობილობების წილი საფრთხეების განაწილებაში ასეთია: SCADA/HMI – 23%, სამრეწველო ქსელური მოწყობილობები – 23%, PLC/RAT – 21%, საინჟირნო (ტპმას-ის) პროგრამული უზრუნველყოფა –18%, სხვები – 15%.

საფრთხეების ტიპობრივი განაწილება ასეთია: ჭარბი უფლებები და პრივილეგიები – 11%, შეტანის არასწორი კონტროლი – 9%, საფრთხეები მეხსიერებასთან მუშაობისას – 8%, გასვლა დანიშნული კატალოგიდან – 7%, და ა.შ. ჯამში, 64% დაუცველობისა შეიძლება გამოყენებული იყოს დისტანციური ზემოქმედებისათვის. დაუცველობების განაწილება რისკების დონეების მიხედვით შემდეგია (CVSS ვერსია 3): მაღალი – 53%, კრიტიკული – 25%, საშუალო - 21%, დაბალი – 1%. ზოგადად, მაღალი დონის რისკები მოქმედებს კომპლექსურად, ისინი ერთდროულად არღვევენ ინფორმაციული უსაფრთხოების სამ ძირითად თვისებას – კონფიდენციალურობას, მთლიანობას და მიღწევადობას. 2018 წელს დაუცველობა იყო 58%. ამათგან, მხოლოდ 4%-ს სჭირდებოდა მაღალი კვალიფიკაცია, დანარჩენი კი ხელმისაწვდომი იყო დაბალი კვალიფიკაციის ბოროტგანმზრახველებისთვისაც კი.

საკითხის აქტუალობიდან გამომდინარე, **ტპმას**-ის უსაფრთხოების საკითხების დამუშავებაში აქტიურად ჩაერთვნენ როგორც კერძო კომპანიები, ისე სახელმწიფო ორგანიზაციები. პუბლიკაციებიდან ირკვევა, რომ **ტპმას**-ის დაპროექტების და გამოყენების მეთოდები საკმაოდ კონსერვატიულია და არ პასუხობს თანამედროვე მოთხოვნებს. უსაფრთხოების მიმართ მოთხოვნები უნდა იყოს ჩამოყალიბებული ტექნიკურ დავალებებში, რეალიზებული – პროექტებში, განხორციელებული – რეალურ ტექნიკურ სისტემებში და დანერგილი – საექსპლუატაციო პირობებში.

აქ მოკლედ შევეხებით იმ ორგანიზაციულ და ტექნიკურ ღონისძიებებს, რომლებიც უნდა განხორციელდეს **ტპმას**-ის მართვის სისტემებში, რათა დაცული იყოს ტექნოლოგიური პროცესების უსაფრთხო მიმდინარეობა. იმ წყაროების ჩამონათვალი საიდანაც აღებულია აქ მოტანილი მონაცემები, მოცემულია სტატიის ბოლოს. საჭიროა, რომ:

1. პირველ რიგში, ტექნოლოგიური ქსელი მაქსიმალურად იყოს იზოლირებული ყველა დანარჩე-

ნისგან. წვდომა ამ ქსელთან უნდა მოხდეს მხოლოდ დემილიტარიზებული ზონიდან.

2. ტექნოლოგიური ქსელის ყველა კვანძი დაცული იყოს შეტევებისაგან დაცვის აქტიური საშუალებებით.

3. ქსელური ეკრანები განთავსდეს ტექნოლოგიური ქსელის საზღვრებთან, გაეწყოს ისინი შორეული წვდომის მოდულებიდან შემოტევის ასარიდებლად.

4. დაცვითი სისტემები განთავსდეს კორპორატიული ქსელის საზღვარზე და მის შიგნით სპამური და ფიშინგური გზავნილების აღსაკვეთად.

5. ანტივირუსული დაცვის საშუალებები განთავსდეს გარე ქსელის საზღვრებზე.

6. აიკრძალოს ტექნოლოგიური ქსელის შიგნით გარე საფოსტო გზავნილების მიღება/გაგზავნა. აიკრძალოს არააუცილებელი საფოსტო გზავნილების მიღება კორპორატიული ქსელიდან.

7. აიკრძალოს არააუცილებელი საერთო საქაღალდეების გამოყენება ტექნოლოგიური ქსელის შიგნით.

8. გაუქმდეს შორეული ადმინისტრირების ყველა არააუცილებელი საშუალება ტექნოლოგიურ ქსელში.

9. გაუქმდეს შორეული ადმინისტრირების ყველა არააუცილებელი საშუალება ტექნოლოგიურ ქსელში, რომელიც მოყვება **ტპმას**-ის პროგრამულ უზრუნველყოფას.

10. თუ აუცილებელი არ არის, გაუქმდეს შემდეგი პროგრამები ტექნოლოგიურ ქსელში:

(ინტერნეტბრაუზერი, სოციალური ქსელის კლიენტები, საფოსტო კლიენტები, MS Office-ის პროგრამები, Adobe პროგრამები, Java Runtime, მედიასაკრავები, სკრიპტული ინტერპრეტატორები - Perl, Python, PHP, არალიცენზირებული პროგრამები).

11. თუ საჭირო არ არის, გამოირთოს Windows Script Host;

12. შესაძლებლობის ფარგლებში შეიზღუდოს SeDebugPrivilege-ის გამოყენება;

13. მომზადდეს პერსონალი კიბერჰიგიენის სფეროში;

14. შეიქმნას სამსახურები სამრეწველო ინფორმაციული სისტემების დასაცავად;

15. რეგულარულად ჩატარდეს ტექნოლოგიური ქსელის ინფორმაციული უსაფრთხოების სისტემის აუდიტი;

16. უზრუნველყოფილი იყოს ტექნოლოგიური ქსელის დაუცველობების დროული აღმოჩენა და ლიკვიდაცია;

17. დაინერგოს ტექნოლოგიური ქსელის კრიტიკული არეების მონიტორინგის ავტომატური და ავტომატიზებული საშუალებები;

18. დაინერგოს ტექნოლოგიურ ქსელში საფრთხეების ინციდენტების რეგისტრაციის და დამუშავების სპეციალიზებული საშუალებები;

19. ახალი **ტპმას**-ის დანერგვის წინ მოხდეს მისი ტესტირება ინფორმაციულ უსაფრთხოებაზე;

20. საფრთხისგან – „ადამიანი შუაში“ დაცვისათვის, ტექნოლოგიური ქსელის შიგნით და საზღვრებზე გამოყენებულ იქნეს ტრაფიკის კრიპტოგრაფიული დაშიფვრა.

21. სადაც საჭიროა, გამოყენებულ იქნეს ტრაფიკის დაშიფვრა ტექნოლოგიური ქსელის კომპონენტებს შორის;

22. ტექნოლოგიურ ქსელში პერსონალის დაშვება მოხდეს ორფაზური აუთენტიფიკაციით;

23. და რაც უმნიშნელოვანესია, მოხდეს ყველა დონის პროგრამული საშუალების რეგულარული განახლება.

3. ვირუსული ჭიაყელა Stuxnet-ის მიერ განხორციელებული შეტევა ირანის ატომურ სადგურზე ბუშერში

ამასწინათ, ირანის ახალი ამბების ოფიციალურმა სააგენტომ განაცხადა, ირანის ატომური ქარხნის ზოგიერთი კომპიუტერული სისტემის ინფიცირების შესახებ Stuxnet კომპლექსური ვირუსით. უფრო ადრე სპეციალისტები აცხადებდნენ, რომ ეს ზიანის მატარებელი კოდი „ჩაკირულია“ სამრეწველო ობიექტების ქვეშ და მაშინვე გამოჩნდნენ ექსპერტები, რომლებიც ამტკიცებდნენ, რომ ვირუსი ზუსტად იმისთვის არის შექმნილი, რომ მწყობრიდან გამოიყვანოს ირანის ატომური ელექტროსადგური. ამ თემაზე სპეკულაცია ხდება მრავალი მასობრივი ინფორმაციის საშუალების მხრიდანაც სერიოზული გამომცემლობიდან დაწყებული „ყვითელი“ პრესით დამთავრებული, მაგრამ, მიუხედავად ამისა, ჯერ კიდევ არ არის დამტკიცებული, რომ Staxnet ჭიაყელა ვირუსი შექმნილია სპეციალურად ირანის ატომური ობიექტებისათვის.

ბუშერის ატომური ელექტროსადგურის დირექცია აცხადებს, რომ თუმცა ვირუსმა შეძლო დაეინფიცირებინა საწარმოს ზოგიერთი კომპიუტერული სისტემა, მას არ მიუყენებია არავითარი ზიანი ქარხნის მთავარი სისტემებისათვის.

ამ დროისათვის არსებობს ექსპერტთა ორი ძირითადი აზრი ამ ვირუსის შესახებ.

1. Stuxnet-ი არ არის შექმნილი მხოლოდ ირანის სამრეწველო ობიექტების დასაზიანებლად;

2. Stuxnet-ი შექმნილია არა ერთი ხაკერის, არამედ სპეციალისტების მთელი ჯგუფის მიერ, რომლებიც შესანიშნავად არიან გათვითცნობიერებულნი კერძო საკუთრებაში არსებულ სამრეწველო პროგრამულ უზრუნველყოფაში.

ეს უკანასკნელი აზრი დაფუძნებულია იმ ფაქტზე, რომ Stuxnet-ს ერთის მხრივ აქვს ძალზე რთული სტრუქტურა, რომლის გაშიფვრისათვის ჯერ კიდევ მუშაობენ ექსპერტები; მეორეს მხრივ Stuxnet კოდში არ არის ინდივიდუალური „ნიშნულები“, რომლებიც დამახასიათებელია ცალკეული პირების მიერ შექმნილი პრაქტიკულად ნებისმიერი პროგრამული უზრუნველყოფისათვის. ზოგადად კი, ალბათობა იმისა, რომ Stuxnet-ი შექმნილია ერთი რომელიმე ჰაკერის მიერ, უახლოვდება ნულს.

იგივე ექსპერტები თვლიან, რომ ისეთი ვირუსის გამოჩენით, როგორიც Stuxnet-ია, მსოფლიოში გაჩნდა ნამდვილად სერიოზული კიბერიარაღი, რომელიც რაიმე საკრედიტო ბარათების ნომრებს კი არ იპარავს, არამედ შეუძლია გამოიწვიოს სერიოზული ავარია მეტად სასშიშ სამრეწველო ობიექტზე. საფრთხის ასეთი ტიპი, იმავე ექსპერტების აზრით არის აბსოლუტურად ახალი და აქედან გამომდინარე, მრავალმა ექსპერტმა დაიწყო პირდაპირი მნიშვნელობით წარმოებების დაშინება იმ მიზნით, რომ მათ დაიწყონ უსაფრთხოების სერიოზული ზომების გატარება.

Stuxnet-მა რუსი სპეციალისტების ყურადღებაც მიიპყრო. ისინი თვლიან, რომ ბოროტმოქმედები შეეცადნენ პროგრამა იმგვარად დაემუშავებინათ, რომ მას მიექცია რაც შეიძლება ნაკლები ყურადღება. Win32/Stuxnet-ის დაინფიცირების მეთოდიც კი უნიკალურია, ვინაიდან პროგრამული უზრუნველ-

ყოფა იყენებს ადრე უცნობ დაუცველობას. გარდა ამისა, „იმის შესაძლებლობა, რომ ვირუსის შეღწევა პერსონალურ კომპიუტერში შესაძლებელია USB დამგროვებლების გზითაც, ქმნის ამ ვირუსის ფართოდ გავრცელების წინაპირობას“. ასეთი კომენტარი გაკეთდა ვირუსული კვლევების და ანალიტიკის ცენტრის – Eset-ის წარმომადგენლობაში. ისინი თვლიან რომ Stuxnet-ის ორიენტაცია მაინცდამაინც ირანის ატომურ ობიექტებზე შეიძლება სრულიად უსაფუძვლო აღმოჩნდეს, რადგან ამ ვირუსმა ჯერ-ჯერობით ყველაზე დიდი გავრცელება ამერიკის შეერთებულ შტატებში პოვა, შემდეგ კი – ირანში. რუსეთი ჯერჯერობით მესამე ადგილზეა ამ ვირუსის გავრცელების თვალსაზრისით.

ამ ფაქტის შესახებ არსებობს სხვა მოსაზრებაც. მაგალითად, გერმანელმა სპეციალისტმა ინფორმაციულ უსაფრთხოებაში რალფ ლენგრენმა დეტალურად შეისწავლა ეს ვირუსი და არაერთი ანალიზის შემდეგ დაასკვნა, რომ ამ ჭიაყელას შექმნის უკან შეიძლება მთელი სახელმწიფოც კი იდგეს და არა რომელიმე ხაკერ-სტუდენტი ან სტუდენტთა ჯგუფი. ლენგრენმა წარმოების ინფორმაციული ტექნოლოგიების უსაფრთხოების ერთ-ერთ კონფერენციაზე დამამტკიცებელ საბუთად მოიყვანა ვირუსის კოდის მონაკვეთების დეტალური ანალიზი და გამოაქვეყნა თავის საიტზე. ძირითადი დასკვნა ასეთია: „Stuxnet-ი არის 100%-ით დამიზნებადი შეტევის იარაღი, რომელიც მიმართულია ჩვეულებრივი სამრეწველო პროცესების დარღვევაზე რეალურ და არა ვირტუალურ სამყაროში“. შესაბამისად, უსაფრთხოების ექსპერტები Stuxnet-ს უწოდებენ პირველ ვირტუალურ სუპერიარაღს, რომელიც შექმნილია რეალური ობიექტების გასანადგურებლად.

ამერიკის სამი უდიდესი სპეციალისტი ინფორმაციულ ტექნოლოგიებში, მათ შორის მაიკლ ასანტეც, ეთანხმება ლენგრენის თეორიას, მაგრამ საგანგებოდ აღნიშნავენ, რომ ვირუსის კოდი ჯერ კიდევ არასაკმარისად არის შესწავლილი, იგი განსაკუთრებით რთულია და მუშაობა მის შესასწავლად გაგრძელდება.

საინტერესოა ისიც, რომ არაერთი სპეციალისტი მივიდა იმ აზრამდე, რომ უსაფრთხოების თვალსაზრისით ირანის ატომური ქარხანა Bushehr-ი არის მთავარი სამიზნე ამ ვირუსისათვის, მაგრამ არ უნდა დაგვავიწყდეს, რომ ეს ვირუსი აღმოჩენილია მთელ მსოფლიოში და არა მხოლოდ ირანში. ვირუსული გამოკვლევებისა და ანალიტიკის Eset-ის ცენტრის ხელმძღვანელობამ წარმოადგინა ამ ვირუსის გავრცელების სტატისტიკა, რომლის თანახმადაც იგი გავრცელებულია შემდეგნაირად:

ირანი – 52,2%
ინდონეზია – 17,4%
ინდოეთი – 11,3%

იგივე წარმომადგენლობა აღნიშნავს, რომ ბუშერი შეიძლება იყოს ამ ვირუსის ერთ-ერთი სამიზნე, მაგრამ არაფერი მიუთითებს იმაზე, რომ ეს სამიზნე ამ ვირუსისათვის იყოს ძირითადი. მაგალითად, გერმანიაშიც კი იყო დაფიქსირებული ამ ვირუსის მიერ რამდენიმე ატომური ელექტროსადგურის დაინფიცირება.

თუ მივიღებთ მხედველობაში, რომ Stuxnet ვირუსი გათვალისწინებულია პირველ რიგში Siemens-ის პროგრამული უზრუნველყოფის მქონე პერსონალური კომპიუტერებისთვის, რომლებიც ჩვეულებრივ გამოიყენება წარმოების პროცესების მართვის

სხვადასხვა სამრეწველო სისტემაში, კონკრეტულად, არა იმდენად მცირე, არამედ საკმაოდ რთულ და სახიფათო საწარმოებში, მაგალითად, თვით ატომურ ქარხნებში. პერსონალურ კომპიუტერებში შეღწევისათვის Stuxnet-ი იყენებს OS Widows-ის სამ დაუცველობას, რომელთაგან დღეისათვის გადაკეტილია მხოლოდ ერთი. Stuxnet კოდი შეიცავს ისეთ მონაკვეთს, რომლებიც თეორიულად აძლევს შესაძლებლობას ბოროტმოქმედს მიიღოს წვდომა პროცესების მართვის სისტემებთან. აქედან გამომდინარე, Stuxnet-ს შეუძლია შეტევა განახორციელოს წარმოების მართვის კომპონენტებზე, ანუ SCADA სისტემაზე, რაც გამოიყენება ქიმიურ, ნავთობქიმიურ, ატომურ მსხვილ და უმსხვილეს საწარმოებში.

4. **SCADA – შეტევის ობიექტი: ტექნოლოგიური პროცესების მართვის ავტომატიზებული სისტემების დაცულობის ანალიზი**

Stuxnet ვირუსის აღმოჩენამ ბუშერში, ატომურ ობიექტებზე, დიდი ხმაური გამოიწვია. დაისვა კითხვა – „ვინ დგას ყოველივე ამის უკან?“ – ამ კითხვაზე ალბათ არ გაეცემა პასუხი რამდენიმე ათეული წლის განმავლობაში. კრიტიკულად მნიშვნელოვანი ინფრასტრუქტურის ობიექტებია დღეისათვის მრავალთათვის დიდი ინტერესის საგანი: კონკურენტი კორპორაციებიდან დაწყებული, მტრულად განწყობილი სახელმწიფოების სპეცსამსახურებით დამთავრებული.

კრიტიკულად მნიშვნელოვანი ინფრასტრუქტურები გულმოდგინედ დაცული ობიექტებია, ამიტომ მათ ტერიტორიაზე შესვლა და რაიმეს შეტანა უკიდურესად გართულებულია. აქედან გამომდინარე, განსაკუთრებულ ინტერესს წარმოადგენს შორიდან შეტევის შესაძლებლობა. დღეისათვის ყოველი სახელმწიფო ადგენს ყველაზე დასაცავი ობიექტების სიას. მიუხედავად იმისა, რომ ეს სია სახელმწიფო საიდუმლოებაა, მაინც აბსოლუტურად ნათელია მათი შემადგენლობა: ელექტროენერგეტიკის ობიექტები, ბირთვული და ატომური დარგები, გაზისა და ნავთობის ტრანსპორტირების საშუალებები, ნავთობქიმიური საწარმოები, სტრატეგიული სამხედრო ობიექტები. რა თქმა უნდა, ამ ობიექტების დიდი ნაწილი ავტომატიზებულია ინფორმაციული ტექნოლოგიების გამოყენებით, რაც კომპლექსურად წარმოადგენს ტექნოლოგიური პროცესების მართვის ავტომატიზებულ სისტემებს (**ტპმას**).

ტიპური **ტპმას**-ის შემადგენლობაში შედის სამი ძირითადი კომპონენტი: დისპეტჩერიზაციის სისტემა (SCADA) (ფიგ. 6), ტელემეტრიული ქვესისტემა და კომუნიკაციის ინფრასტრუქტურა მონაცემთა გადაცემის სამრეწველო პროტოკოლების გამოყენებით. ხშირად საზღვარგარეთ ტერმინი **ტპმას**-ი გამოტოვებულია და ლაპარაკობენ მხოლოდ SCADA სისტემებზე, თუმცა მნიშვნელოვანია გვახსოვდეს, რომ მხოლოდ დისპეტჩერიზაციას არ შეუძლია ინტერაქტიულად მართოს მთელი სისტემური პროცესები.

როგორი ინსტრუმენტები დაგვჭირდება **ტპმას**-ის უსაფრთხოების ანალიზისთვის, თუ მხედველობაში მივიღებთ, რომ საქმე გვაქვს ტექნოლოგიური პროცესების დისპეტჩერიზაციისა და მართვის სისტემებთან? აქ გასათვალისწინებელია, რომ 60% ცნობილი **ტპმას**-ისა იყენებს ტრადიციულ Windows, Linux პლატფორმებს.

აუცილებლობის შემთხვევაში გამოიყენება რეალური დროის პლატფორმები, ისეთი როგორიც QNX, რომლებიც იძლევა ამა თუ იმ ოპერაციის მო-

ცემული დროის ინტერვალში შესრულების გარანტიას, თუმცა ეს სისტემები უფრო მეტად გამოიყენება სამხედრო დანიშნულების ობიექტებში (საბორტო მართვა).

დღეისათვის არსებობს არცთუ ისე ბევრი ვიწრო-სპეციალიზებული პროგრამული საშუალება **ტპმას**/ SCADA -ს უსაფრთხოების ანალიზისთვის:

ფიგ. 6. დისპეტჩერიზაციის SCADA სისტემა ბუშერის აეს-ში

- პერსონალური კომპიუტერი „SCADA -აუდიტორი“ ტექნოლოგიური ქსელების, **ტპმას/ SCADA**-ს დაცულობის ანალიზის სკანერი;
- Teenable Nessus-ი, რომელიც შეიცავს SCADA სისტემის და კომერციული პროგრამული ლოგიკური კონტროლერების მწკრივის შემოწმების რამდენიმე მოდულს;
- Rapid7 Metasploit Project (აქ უკვე ყველაზე მწირი მდგომარეობაა: განყოფილებაში „exploits/scada/“ სულ რამდენიმე წყვილი ვიწრო მიმართულების უტილიტაა).

ბუნებრივია, რომ ამ სპეციალიზებული პროგრამული უზრუნველყოფის გარდა გამოიყენება ტრადიციული ინსტრუმენტები, მაგ. ქსელური nmap სკანერი. ამასწინათ მასში აგრეთვე შეიტანეს პლაგინი, რომელსაც შეუძლია აღმოაჩინოს Stuxnet-ით დაინფიცირებული კვანძი.

5. **როგორ აღმოვაჩინოთ Stuxnet-ით დაინფიცირებული კვანძი**

NMAP-ის **(Network Mapper)** ახალ ვერსიაში შეტანილია საინტერესო პლაგინი, რომელიც დაწერილია NMAP Scripting Engine დაპროგრამების ენაზე LUA. მისი სახელია – „stuxnet-detect“.

- ამ პროდუქტით რომელიმე კვანძის გამოკვლევა – იმის შესახებ, არის თუ არა მასში ვირუსი stuxnet SMB - სესიის გავლით, ძალზე მარტივია: Nmap -script stuxnet-detect –p 445 <host>.

გარდა ამისა, დაზიანებული კვანძის აღმოჩენისთვის შეიძლება სკანერის გამოყენება, რომელიც შექმნეს Trend Micro კომპანიის სპეციალისტებმა. როგორ მუშაობს ეს სკანერი და ზოგადად, როგორ მუშაობს stuxnet-ი? Stuxnet-ი არეგისტრირებს თავის RPC სერვერს შიგა და გარე ურთიერთქმედებისათვის, დაზიანებულ კვანძებთან ცალკე კვანძის სახით. RPC სერვერის ფუნქციონალი აწყობილია ჭიაყელას

ვერსიისა და, აგრეთვე, განახლების ფუნქციის შემოწმებაზე (ახალი ეგზემპლარების ჩატვირთვა). შესაბამისი RPC გამოძახებები შესაძლებელია შესრულდეს ამ „სამრეწველო“ ბაგნეტის მართვის ცენტრიდან. ცენტრი გამოსცემს ბრძანებას ვერსიის (0x00) შემოწმების შესახებ. წინასწარ მოწმდება SMB-over_TCP (TCP 445) სამსახურთან ხელმისაწვდომობა, რის შემდეგაც ხდება სივიწროვეთა გამოკვლევა, რაც ჩადებულია Stuxnet-ის ამ ვერსიაში (მაგალითად, MS10-061). მე-2 მეთოდია „ჩაყვინთული“ ბოროტმოქმედი Stuxnet-ის კოდის მოძებნა ამოცანათა დამგეგმვაში. ამ მეთოდიკის საფუძველზე მუშაობს Trend Micro სკანერი.

დასკვნა

ოპერატორის სადგურის დაინფიცირება ვირუსით ნაკლებად ალბათურია, მაგრამ თუ მაინც მოხდა, არავითარ ზიანს ეს მოვლენა არ გამოიწვევს. რა თქმა უნდა, არსებობს შემთხვევები, როდესაც ოპერატორები გვერდს უვლიან აკრძალვებს და აყენებენ თავის სადგურებზე კომპიუტერულ თამაშებს ან გადიან ინტერნეტსივრცეში, მაგრამ ამის აღკვეთა სწრაფად ხდება სხვადასხვა ადმინისტრაციული მეთოდის გამოყენებით.

თუ დავუშვებთ, რომ არსეობს სპეციალიზებული ვირუსი, რომელმაც იცის მთელი სისტემის ფუნქციონირების თავისებურებანი და შეუძლია ჰიპოთეტურად მართოს ტექნოლოგიური პროცესი, რამაც შეიძლება ნეგატიური შედეგები გამოიწვიოს, ამ შემთხვევაშიც კი, ანუ ავარიული სიტუაციის წარმოშობის შემთხვევაში, ამუშავდება **ასად** სისტემა (რომელიც არ იმართება ოპერატორის სადგურიდან) და გადაიყვანს წარმოებას უსაფრთხო მდგომარეობაში. რა თქმა უნდა, ამან შეიძლება გამოიწვიოს წარმოებისათვის მილიონობით ზარალი (წარმოების გაჩერება), მაგრამ ნებისმიერ შემთხვევაში არ მოხდება ტექნოგენური კატასტროფა.

თუ ვილაპარაკებთ საინჟინრო სადგურ **ასად**-ის ვირუსით დაინფიცირებაზე, მაშინ ეს უნდა იყოს სუპერინტელექტუალური ვირუსი, რომელიც თვითონ გადააპროგრამებს **პლკ**-ს, თანაც ისეთნაირად, რომ ის მწყობრიდან საჭირო დროს გამოვიდეს, რა თქმა უნდა, ეს არ არის ყველა ის ფაქტორი რომელიც გადააქცევს საინჟინრო სადგურ **ასად**-ის დაინფიცირებას ნაკლებად ალბათურ ხდომილებად, მაგრამ ამ ღონისძიებებს შეიძლება დაემატოს რამდენიმე მოქმედება, მაგალითად **პლკ**-ებში ჩატვირთული პროგრამების და პაროლის გამუდმებულად შემოწმება. თანამედროვე **ტპმას**-ას, რა თქმა უნდა, საფრთხეს უქმნის ვირუსები და სხვა მაღალტექნოლოგიური პრობლემები, როგორიცაა: ოპერატორის სადგურის გადასვლა ბანალურ BSOD-ში, მაგრამ ისინი არ არის ისეთი კრიტიკული, როგორც ბევრს ჰგონია. უნდა გვახსოვდეს, რომ სისტემის უსაფრთხოებას თვალს ადევნებს **ასად** სისტემები, რომლის კონფიგურირებასაც უდგებიან მთელი სერიოზულობითა და სიფრთხილით.

ლიტერატურა

1. Journal Hacker. (2011, July 8). *SCADA at Gunpoint: Security Analysis of an Automated Process Control System.* Habr.Com. https://habr.com/ru/company/xakep/blog/123672/

2. Stuxnet таки добрался до иранского ядерного завода в Бушере/26 сентября 2010
3. Agadzhanov, M. (2010, September 26). *Stuxnet Reached to Iranian Nuclear Plant in Bushehr.* Habr.Com. https://habr.com/ru/post/104973/
4. *Modern Automated Process Control System.* (2010, October 4). Habr.Com. https://habr.com/ru/post/105375/ https://habr.com/ru/post/105375/

UDC 681.3.06
SCOPUS CODE 1802
https://doi.org/10.36073/1512-0996-2021-4-46-61

Analysis of the Security of Modern Automated Technological Processes Control Systems: Attack on a SCADA Object

Jemal Grigalashvili Department of Control Systems, Georgian Technical University, Georgia, 0160, Tbilisi, 77 M. Kostava str.
E-mail: j.grigalishvili@gtu.ge

Zaur Jojua Department of Computer Engineering, Georgian Technical University, Georgia, 0160, Tbilisi, 77 M. Kostava str.
E-mail: jojuazauri@yahoo.com

Nino Jojua Department of Computer Engineering, Georgian Technical University, Georgia, 0160, Tbilisi, 77 M. Kostava str.
E-mail: jojua_nina@gmail.com

Reviewers:

K. Kotrikadze, Professor, Faculty of Informatics and Control Systems, GTU
E-mail: ketino27@gmail.com
K. Odisharia, Professor, Faculty of Informatics and Control Systems, GTU
E-mail: o_korneli@yahoo.com

Abstract. (……) Modern automated technology process control systems and the chances of attacks on them are examined in this article. It studies worm virus, Stuxnet, and its detection at the Bushehr Nuclear Power Plant. It also analyzes ways of carrying out attacks on critically important objects, and provides analytical tools for the security of technological process systems. The ways for discovering nodes compromised by the Stuxnet virus are proposed. The article considers technological network of typical topology and its typical vulnerabilities; it analyzes the Modbus protocol, the routing system, and passwords on Cisco routers.

Keywords: Bushehr Nuclear Power Plant; Cisco router; Modbus protocol; passwords; routing system; SCADA; Stuxnet virus; the security of modern automated technology process control systems.

UDC 681.3.06
SCOPUS CODE 1802
HTTPS://DOI.ORG/10.36073/1512-0996-2021-4-46-61

Анализ безопасности современных автоматизированных систем управления технологическими процессами: атака на объект SCADA

Джемал Григалашвили Департамент систем управления, Грузинский технический университет, Грузия, 0160, Тбилиси, ул. М. Костава 77
E-mail: j.grigalishvili@gtu.ge

Заур Джоджуа Департамент компьютерной инженерии, Грузинский технический университет, Грузия, 0160, Тбилиси, ул. М. Костава 77
E-mail: jojuazauri@yahoo.com

Нино Джоджуа Департамент компьютерной инженерии, Грузинский технический университет, Грузия, 0160, Тбилиси, ул. М. Костава 77
E-mail: jojua_nina@gmail.com

Рецензенты:

К. Котрикадзе, профессор факультета информатики и систем управления ГТУ
E-mail: ketino27@gmail.com

К. Одишария, профессор факультета информатики и систем управления ГТУ
E-mail: o_korneli@yahoo.com

Аннотация. (……) В статье рассматриваются современные автоматизированные технологические системы управления процессом и вероятность кибератак на них. Изучается вирус Stuxnet и его обнаружение на Бушерской атомной электростанции. Также анализируются способы совершения нападений на критически важные объекты и предоставляются аналитические инструменты для обеспечения безопасности систем технологических процессов. Предложены способы обнаружения узлов, скомпрометированных вирусом Stuxnet. Более того, в статье рассматривается технологическая сеть типичной топологии и ее типичные уязвимости; анализируется протокол Modbus, система маршрутизации и пароли на маршрутизаторах Cisco.

Ключевые слова: АЕС «Бушер»; безопасность современных автоматизированных систем управления технологическими процессами; вирус Stuxnet; маршрутизатор Cisco; протокол Modbus; пароли; система маршрутизации; SCADA.

განხილვის თარიღი 04.06.2021
შემოსვლის თარიღი 21.06.2021
ხელმოწერილია დასაბეჭდად 28.12.2021