DOI: 10.61760/18290108-ehp24.2-71

ՊԱՇՏՊԱՆԱԿԱՆ ՈԼՈՐՏՈՒՄ ԿԵՂԾ ՑԱՆՑԱՅԻՆ ԵՆԹԱԿԱՌՈՒՑՎԱԾՔՈՒՄ ՆԵՅՐՈՆԱՅԻՆ ՑԱՆՑԻ ԿԻՐԱՌՄԱՆ ՄՈԴԵԼԻ ՀԵՏԱԶՈՏՈՒԹՅՈՒՆ*

Թ. Վ. ՋԱՄՂԱՐՅԱՆ, փոխգնդապետ, տեխնիկական գիտությունների թեկնածու, ՀՀ ՋՈՒ-ի ԳՇ կապի և ԱԿՀ վարչության կապի անվտանգության և գաղտնագրված կապի բաժնի պետի տեղակալ, Թ. Ն. ՇԱՀՆԱԶԱՐՅԱՆ, գեներալ-մայոր, ՀՀ ՋՈՒ-ի ԳՇ օպերատիվ գլխավոր վարչության պետ – ՋՈՒ-ի ԳՇ պետի տեղակալ

Համառոտ նկարագրություն

Հոդվածում ներկայացված են կեղծ ցանցային ենթակառուցվածքի (ՑԵ) կառավարման համար մեքենայական ուսուցման մեթոդների կիրառման հաշվարկումների ու թեստերի արդյունքները: Կեղծ ցանցային ենթակառուցվածքի և դրանում շրջանառող տվյալների կառավարումը կատարվել է գեներատիվ-մրցակցային ցանցի հիման վրա[1]: Որպես գնահատման պարամետրներ ընտրվել են ճշտությունը *(accuracy),* ճշգրտությունը *(precision),* զգայունությունը *(recall)* և ուրույնությունը (սպեցիֆիկությունը, *specificity):* Որպես գեներատիվ-մրցակցային ցանցի կիրառման որակի գնահատում ընտրվել է նվազագույն խտրանքային շեմի (ՆԽՇ, *Fscore,* կատարողականության գնահատական) չափանիշը: «Հայպեր-Վի» *(“Hyper-V”)* հիպերվիզորի հիման վրա կատարվել է տարատեսակ գրոհների մոդելավորում: Կեղծ ցանցային ենթակառուցվածքը կառավարող գեներատիվ-մրցակցային ցանցը միացված էր մեքենայական ուսուցմամբ օժտված՝ ներխուժումների հայտնաբերման համակարգին կեղծ ենթակառուցվածքում շրջանառող տվյալների հավաքածուների ստոխաստիկ արժեքների գեներացման համար:

Ներածություն

Վեցերորդ սերնդի պատերազմներում արդեն վճռորոշ դերը պատկանում է ոչ թե մեծաքանակ ցամաքային զորքերին ու միջուկային զենքին, այլ գերճշգրիտ և նոր ֆիզիկական սկզբունքներով գործող զենքին: Այսօր զինված պայքարի միջոցներում տեղի է ունենում կիրառվող գերճշգրիտ միջոց-

* Հոդվածը ներկայացվել է 20.03.2024՝ ռուսերեն: Հոդվածի գրախոսությունը ստացվել է 06.06.2024:

[1] Գեներատիվ-մրցակցային ցանցի վերաբերյալ առավել հանգամանորեն տես *Թ. Վ. Ջամղարյան,* Ներխուժումների հայտնաբերման համակարգի արդիականացում գեներատիվ մոդելի կիրառմամբ: «ՀԲ», 2021, հմ. 2:

ների թվի անընդհատ աճում: Արագությունը, համաժամանակությունը, կառավարման արագագործությունը դառնում են ռազմական օպերացիաների հաջողությունը պայմանավորող վճռորոշ գործոններ[2]: Այս ամենը հանգեցնում է կապի համակարգի կայունությանը ներկայացվող պահանջների խստացմանը, ինչպես նաև դրա վրա հաջող գրոհի հնարավոր հետևանքների նվազեցմանն ուղղված լուծումների մշակմանը: Անհրաժեշտ է նաև կանխապես ստեղծել այնպիսի պայմաններ, երբ կապի համակարգի բաղադրիչներից մեկի՝ ցանցային ենթակառուցվածքի (ՑԵ) վրա հաջող գրոհի համար չարագործին կպահանջվի ահռելի հաշվողական ռեսուրս: Պաշտպանության ենթակառուցվածքային համակարգի բացազատման ժամանակ, տարատեսակ պաշտպանապատների (ֆայերվոլների), ներխուժումների հայտնաբերման ու կանխման համակարգերի *(IDS, Intrusion Detection System, IPS, Intrusion Prevention System)*[*], «ԱՏԻԿ» (Անվտանգային տեղեկույթի և իրադարձությունների կառավարման, *"SIEM", Security Information and Event Management)* համակարգի և այլ համակարգերի հետ մեկտեղ, նույնպես բացազատվում է «Հանիփոտ» *(Honeypot)*[**] կեղծ ցանցային ենթակառուցվածքը: Արդեն գոյություն ունեցող մոդելների *(CIA*[***]*, STRIDE*[****]*, 5A*[*****]*,* Փարկերի հեքսադ և այլն) հիման վրա «սպառնալիքի

[2] Տես *С. И. Макаренко, М. С. Иванов.* Сетецентрическая война. Принципы, технологии, примеры и перспективы. СПб., 2018, сс. 91–92:

[*] Ներխուժումների հայտնաբերման համակարգը *(IDS)* այնպիսի ծրագրային ու ապարատային միջոցների համախումբ է, որոնք նախատեսված են իրենց վստահված ռեսուրսների օգտագործման վերլուծության, համակարգչային ցանցում կամ առանձին գլխավոր համակարգում չթույլատրված վնասաբեր ակտիվության հայտնաբերման համար: Ներխուժումների կանխման համակարգը *(IPS)* ծրագրային արգասիք կամ սարքավորում է, որը նախատեսվում է համակարգչային ցանցում կամ առանձին սարքի մեջ հավանական վնասակար ակտիվության կանխման համար (տես *О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова.* Обнаружение вторжений в компьютерные сети (сетевые аномалии). М., 2022, сс.15–18):

[**] *«Honeypot»*-ը հատուկ խոցելի կամ սխալ կերպով փոխդասավորված համակարգ է, որը դիտավորյալ կերպով բաց է գրոհների համար և ծառայում է որպես խայծ կիբեռհանցագործների համար՝ միևնույն ժամանակ գտնվելով տեղեկատվական անվտանգության մասնագետների անընդհատ հսկողության տակ (տես «Ханипот (honeypot)». Энциклопедия «Касперского» (https://encyclopedia.kaspersky.ru/glossary/honeypot/)):

[***] *«CIA»*-ը (գաղտնիություն *(Confidentiality)*, ամբողջականություն *(Integrity)*, հասանելիություն *(Availability)*) տեղեկատվական անվտանգության մոդել է (տես *W. Stallings.* Cryptography and Network Security. Principles and Practice. Fifth edition. Prentice Hall, 2011, PP. 10–14; *J. Saltzer, M. Schroeder*. The Protection of Information in Computer Systems. Fourth ACM Symposium on Operating System Principles (October 1973). Revised version. "Communications of the ACM", July 1974, Vol. 17, Issue 7):

[****] *«STRIDE»*-ը (նենգափոխում *(Spoofing),* տվյալների փոփոխում *(Tampering),* պատասխանատվությունից հրաժարում *(Repudiation),* տեղեկույթի հրապարակում *(Information Disclosure),* սպասարկման մերժում *(Denial of Service*), արտոնությունների կալնում *(Elevation of Privilege))* տեղեկատվական անվտանգության համակարգ է:

[*****] *«5A»*-ն (վավերացում *(Authentication),* թույլտվություն *(Authorization),* հասանելիություն *(Availability)*, նույնացում *(Authenticity),* ընդունելիություն *(Admissibility))* տեղեկատվական անվտանգության մոդել է:

մոդելի» կառուցումը կարող է նվազեցնել ՑԵ-ի «գրոհի մակերեսը», բայց ի վիճակի չէ լիովին համահարթելու սպառնալիքը: Կեղծ ցանցային ենթակառուցվածքի կիրառումը պայմանավորված է այն բանով, որ «անընդհատ ժամանակ» ունեցող չարագործն ունակ է վերլուծելու ՑԵ-ի ծրագրատեխնիկական կառուցվածքը և բացահայտելու դրանում առկա այն տարատեսակ խոցելիությունները, որոնք անհրաժեշտության դեպքում կարելի է օգտագործել և չհայտնաբերվել: Կեղծ ցանցային ենթակառուցվածքի կիրառման ժամանակ լուծումները թե՛ ֆիզիկական սարքեր են, թե՛ ծրագրային միջավայրներ, որոնք գործում են երևակայացման (վիրտուալացման) տարբեր միջավայրներում: Առավել հաճախ օգտագործվում են այն լուծումները, որոնք երևակայական (վիրտուալ) միջավայրում գործում են ծրագրայնորեն որոշարկվող ցանցերի *(software-defined networking, SDN)* հիմքի վրա: Գոյություն ունեցող կեղծ ցանցային ենթակառուցվածքների հիմնական թերությունը սակավ դինամիկան է (ինչպես տեղաբանական վերադասավորման դեպքում, այնպես էլ տվյալների շրջանառության ոլորտում[*]), ինչը չարագործին հնարավորություն է տալիս համապատասխան վերլուծության հիման վրա հասկանալու, որ ՑԵ-ում կա կեղծ ցանցային ենթակառուցվածք, և գրոհի վեկտորը տեղափոխելու միայն ՑԵ-ի նշանակալի բաղադրատարրի վրա: Իրական ՑԵ-ից կեղծ ցանցային ենթակառուցվածքի խնդիրը լուծելու համար տարբեր հետազոտողներ օգտագործում են տարբեր լուծումներ. մասնավորապես՝ շվեյցարական «Նետսեկ» *(Netsec)* ֆիրմայի մշակած «Սպեկտեր» *(Specter)* ծրագրային ապահովումը (ԾԱ)[3], լինելով ցածր մակարդակի փոխազդեցությամբ «Հանիփոտ»[4], այսինքն՝ առանց ցանցի 1:1 էմուլացիայի, հնարավորություն է տալիս ծավալելու կեղծ ցանցային ենթակառուցվածք, բայց միայն ծառայությունների շրջանակներում: Կեղծ ենթակառուցվածքի «Փրոքսիփոտ» *(“Proxypot”)* ծրագրային ապահովումը հնարավորություն է տալիս ծավալելու կեղծ ենթակառուցվածք տարբեր սպամ-գրոհների դեմ պայքարելու համար, քանի որ ՑԵ-ի նմանարկմամբ հնարավորություն է տալիս ստեղծելու նրա պատճենի արտատպումը՝ սպամի աղբյուրները վերաուղղորդելով դեպի կեղծ ենթակառուցվածք: Մյուս լուծումները («Հանիփոտ», «ՀոսՏիՁ» *(HosTaGe),* «Փենտբոքս» *(Pentbox))* հնարավորություն են տալիս դասավորելու կեղծ ՑԵ-ն ըստ տարբեր խնդիրների, հաղորդակարգերի նմանարկումից մինչև ծրագրային միջավայրների ու ծառայությունների նմանարկում: Դրանց թվում կան ինչպես բարձր, այնպես էլ ցածր մակարդակի փոխազդեցությամբ լուծումներ: Մի շարք աշխատանքներում[5] ներկայաց-

[*] Շրջանառող են կոչվում այն տվյալները, որոնք փոխանցվում են, ընդունվում և պահպանվում:

[3] Տես «Փրոքսիփոտ» ծրագրային ապահովման ներբեռնման էջը (https://proxypot.org/download.html):

[4] Տես “What is SPECTER?”. “Specter” (http://gabiam.com/software/laura_chapelle/Software/specter/):

[5] Տես *Niels Provos.* A Virtual Honeypot Framework. Proceedings of the 13th USENIX Security Symposium. San Diego, CA, USA, 9–13 August 2004 (https://www.usenix.org / legacy / publications /library/ proceedings/sec04/tech/full_paper/provos/

ված են այլ լուծումներ, մասնավորապես՝ ապարատայինից մինչև ծրագրային, և/կամ այնպիսիք, որոնք հնարավորություն են տալիս ինչպես վերադասավորելու կեղծ ցանցային ենթակառուցվածքը, այնպես էլ փոփոխելու դրանում շրջանառող տվյալները: Սակայն փոխդասավորության ու փոխանցվող տվյալների վերադասավորումը որոշարկելի է, ինչը հնարավորություն է տալիս հակառակորդին N թվով բազմակրկնություններից (իտերացիաներ) հետո ՑԵ-ում հայտնաբերել կեղծ ցանցային ենթակառուցվածքը: Առանձին հարց է տիրույթների ստեղծման ալգորիթմներով[*] (ՏՍԱ, *DGA)* գեներացված կեղծ տիրույթների ներմուծումը և կեղծ ցանցային ենթակառուցվածքի օպերատորի արձագանքը նման գրոհին: Մեծ թվով տարատեսակ ՏՍԱ տիրույթներ գեներացնելով և դրանք հաղորդակցման ընդհանուր հոսքի մեջ ներմուծելով՝ չարագործներն սկսում են դիտումը: Կեղծ ցանցային ենթակառուցվածքների համար տվյալ իրադարձությունները գեներացվում են այնպես, ինչպես և իրական ՑԵ-երի համար, սակայն կեղծ ցանցային ենթակառուցվածքի սակավ դինամիկության հետևանքով իրադարձությունների այն խմբերը, որոնք արձագանք են արտաքին ապակառուցողական ներգործություններին, նույնպես բազմակիորեն կրկնվում են: Նման եղանակը չարագործին հնարավորություն է տալիս ՑԵ-ում հայտնաբերելու կեղծ ցանցային ենթակառուցվածքը: Մեքենայական ուսուցման մեթոդների զարգացումը նոր մակարդակի է հասցրել պաշտպանության ու հարձակման միջոցները, քանի որ այդ ուսուցումը, ի տարբերություն որոշարկված համակարգերից, տրամադրում է ոչ միայն զուտ արժեքը՝ հիմնված ֆիքսված մուտքային/մշակվող տվյալների վրա, այլև պարունակում է ստոխաստիկ տարր, որը հնարավորություն է տալիս ամեն անգամ տրամադրելու նոր արժեք[6]: Տվյալ լուծումը կիրառելի է նաև կեղծ ցանցային համակարգի համար: Արդիական է դառնում մեքենայական ուսուցման մեթոդների կիրառումը կեղծ ցանցային ենթակառուցվածքի կառավարման համար: Տարբեր հետազոտողներ դիտարկում են մեքենայական ուսուցման մեթոդների օգտագործումը կեղծ ցանցային

provos.pdf); *Abhishek Mairrh, Debabrat Barik, Kanchan Verma, Debasish Jena.* Honeypot in network security: a survey. Proceedings of the 2011 International Conference on Communication, Computing & Security. Odisha, India, 12–14 February 2011, PP. 600–605 (https://www.researchgate.net/publication/220846415_Honeypot_in_ network_security_A_survey); *L. Spitzner.* Honeypots: catching the insider threat. Proceeding of 19th Annual Computer Security Applications Conference. Las Vegas, NV, USA, 2003, PP. 170–179 (https://doi.org/10.1109/CSAC.2003.1254322); *Jan Gerrit Göbel, Andreas Dewald.* Client-Honeypots: Exploring Malicious Websites. München, 2011 (https://doi.org/101524/9783486711516):

[*] Տիրույթների ստեղծման ալգորիթմները *(DGA, Domain Generation Algorithms)* այն ալգորիթմներն են, որոնք օգտագործում է վնասաբեր ծրագրային ապահովումը, որպեսզի ստեղծի մեծ թվով կեղծ-պատահական տիրույթային անուններ, որոնք հնարավորություն են տալիս կապ հաստատելու կառավարվող հրամանատվական կենտրոնի հետ:

[6] Մեքենայական ուսուցման վերաբերյալ առավել հանգամանորեն տես *Թ. Կ. Ջամղարյան,* Կիբեռոլորտում ներխուժումների հայտնաբերման համակարգերում մեքենայական ուսուցման կիրառման որոշ խնդիրների վերլուծություն: «ՀՔ», 2023, հմ. 1:

ենթակառուցվածքում[7]: Սակայն օգտագործվող մեթոդների թվաքանակը սահմանափակվեց նեյրոնային ցանցերի կիրառմամբ միայն իրադարձությունների գեներացման համար: Մեքենայական ուսուցմամբ ներխուժումների հայտնաբերման համակարգերի հետ հետադարձ կապը ոչ միշտ է եղել: Տվյալ սահմանափակումը կեղծ ցանցային ենթակառուցվածքներում ներխուժումների հայտնաբերման որոշարկումային համակարգերի կիրառման և, որպես կանոն, անցանկալի իրադարձությանը հենց ներխուժումների հայտնաբերման համակարգերի կրկնվող արձագանքումների հետևանք է:

Այս ամենի բերումով առաջանում են միայն մեքենայական ուսուցմանը բնորոշ նոր խնդիրներ, որոնցից է, օրինակ, մեքենայական ուսուցման տարբեր պարամետրների, մասնավորապես՝ ճշտության, ճշգրտության, զգայունության և ուրույնության միջև հաշվեկշիռը գտնելու խնդիրը: Նեյրոնային ցանցերի կիրառմամբ կեղծ ցանցային ենթակառուցվածքների ծավալման ժամանակ կարևոր խնդիր է երկակի (բինար) դասակարգչի տրված չափանիշների միջև հաշվեկշիռ գտնելը: Սույն հետազոտությունում կեղծ ցանցային ենթակառուցվածքում նեյրոնային ցանցի կիրառման դեպքում որպես հաշվեկշիռը պայմանավորող չափագիր վերցված է F_{β_2} – չափը (1)[8].

$$F_{\beta_2} = \frac{(\beta^2+1)\,(\text{ճշգրտություն}) * \text{զգայունություն}}{(\beta^2\,\text{ճշգրտություն} + \text{զգայունություն})}\ , \qquad (1)$$

որտեղ β-ն գործակից է, որը ցույց է տալիս ճշգրտության նշանակալիությունը զգայունության նկատմամբ կամ հակառակը:

Խնդրադրում. մշակել այնպիսի մոդել, որը F_{β_2} – չափի նվազագույն դիսկրիմինացիոն դեպքում միավորի նեյրոնային ցանցը կեղծ ցանցային ենթակառուցվածքի հետ.

Սահմանային պայմաններ.

1. գեներատիվ-մրցակցային ցանցը չպետք է ստեղծի այնպիսի իրադարձություններ, որոնք հանգեցնեն այն բանին, որ վստահելի միջերեսից մեքենայական ուսուցմամբ օժտված՝ ներխուժումների հայտնաբերման

[7] Տես *Muris Sladić, Veronica Valeros, Carlos Catania, Sebastian Garcia.* LLM in the Shell: Generative Honeypots (https://doi.org/10.48550/arXiv.2309.00155); *Meng Wang, Javier Santillan, Fernando Kuipers.* ThingPot: an Interactive Internet-of-Things Honeypot (https://doi.org/10.48550/arXiv.1807.04114); *Shawn Shan, Emily Wenger, Bolun Wang, Bo Li, Haitao Zheng, Ben Y. Zhao.* Gotta Catch'Em All: Using Honeypots to Catch Adversarial Attacks on Neural Networks (https://doi.org/10.1145/3372297.3417231); *Yuntao Wang, Zhou Su, Abderrahim Benslimane, Qichao Xu, Minghui Dai, Ruidong Li.* Collaborative Honeypot Defense in UAV Networks: A Learning-Based Game Approach (https://doi.org/10.48550/arXiv.2211.01772); *Volviane Saphir Mfogo, Alain Zemkoho, Laurent Njilla, Marcellin Nkenlifack, Charles Kamhoua.* AIIPot: Adaptive Intelligent-Interaction Honeypot for IoT Devices (https://doi.org/10.48550/arXiv.2303.12367); *Marcin Nawrocki, John Kristoff, Raphael Hiesgen, Chris Kanich, Thomas C. Schmidt, Matthias Wählisch.* SoK: A Data-driven View on Methods to Detect Reflective Amplification DDoS Attacks Using Honeypots (https://doi.org/10.48550/arXiv.2302.04614):

[8] Տես “Encyclopedia of Machine Learning”. Ed. by Claude Sammut, Geoffrey I. Webb. Springer 2011, PP. 397:

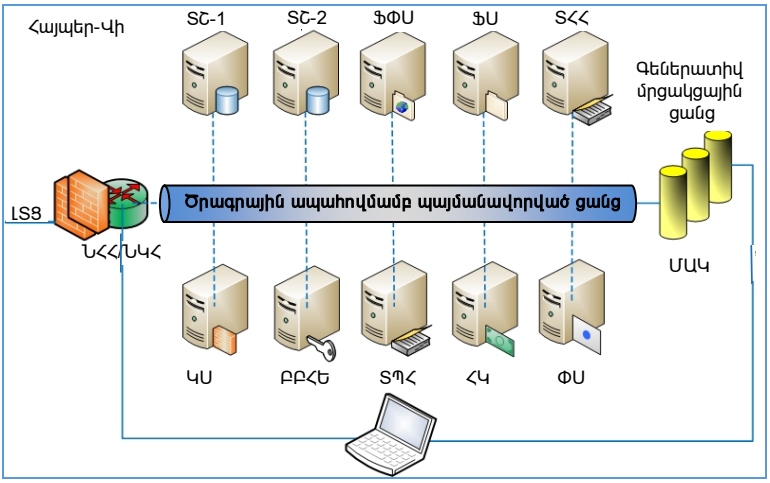
համակարգը գործարկվի ճշմարտորեն – դրական *(true positive)*,

2. կեղծ ցանցային ենթակառուցվածքում գեներատիվ-մրցակցային ցանցի երկրորդ տեսակի սխալների թիվը չպետք է գերազանցի մեքենայական ուսուցմամբ օժտված՝ ներխուժումների հայտնաբերման համակարգի երկրորդ տեսակի սխալների թիվը:

Սույն հետազոտության գիտական նորույթն այն է, որ $F_{նիշ_2}$ ՑԵ-ում $F_{նիշ_2}$-ի նախապես հաշվարկված արժեքով հիմքի վրա շրջանառող տվյալների նոր եզակի հավաքածուների ձևավորման համար կիրառվել է գեներատիվ-մրցակցային ցանց*:

Գիտափորձի նկարագրություն

Երևակայական միջավայրում մեծ արտադրողականությամբ կլաստերների *(“High Performance Clusters”, HPC)* հիմքի վրա տեղակայվել է «Վինդոուզ Սերվեր 2019» *(“Windows Server 2019”)* օպերացիոն համակարգի (ՕՀ) բացազատված կեղծ ցանցային ենթակառուցվածք ներառող «Հայպեր-Վի»՝ երևակայացման ներբեռնված դերով (նկ. 1):



Նկ. 1. Երևակայական միջավայրում բացազատված կեղծ ենթակառուցվածքի մոդել

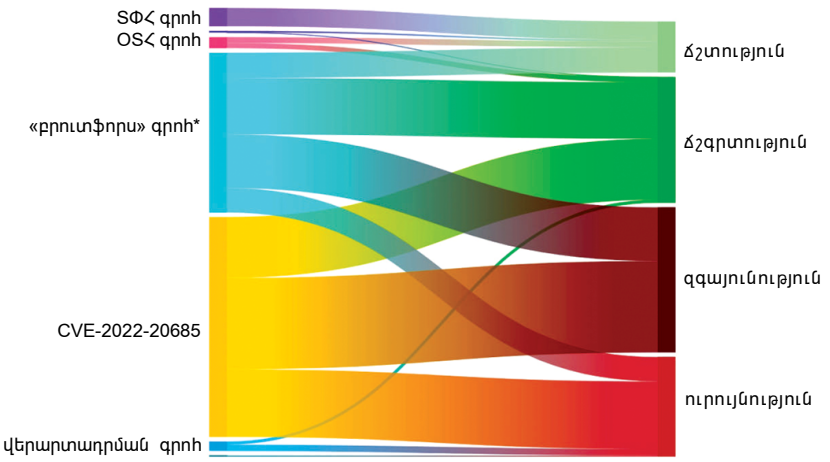
Տիրույթի հիմնական ու պահուստային հսկիչներ *(Primary and Secondary Domain Controller, PDC, SDC)*, ֆայլային սերվեր *(File Server)*, ֆայլերի փոխանցման սերվեր *(FTP Server)*, պրոքսի սերվեր *(Proxy Server)*, բաց բանալիների հավաստագրման ենթակառուցվածք *(Public Key Infrastructure, PKI)*, հավաստիացման կենտրոն *(Certification Authority, CA)*, փոստային սերվեր, մեքենայական ուսուցմամբ օժտված՝ ներխուժումների հայտնաբերման համակարգ և ներխուժումների հայտնաբերման ու կանխման «Սնորտ» (*«Snort»)* համակարգ (սրանում դիտավորյալ չի չեզոքացվել *CVE-2022-20685* խոցելիությունը), տվյալների շտեմարանի սերվերը *(DB-1, DB-2)*:

* Մեր կատարած համալիր հետազոտության լրիվ նկարագրությունը և արդյունքները տես “Popular repositories” (https://github.com/T-JN):

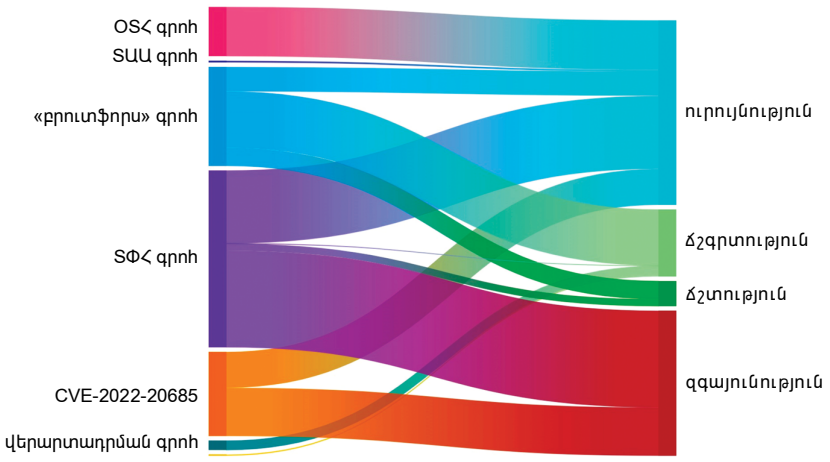
Առանձին բացազատվել է նաև «Ուբունտու 20.04» *("Ubuntu 20.04")* ՕՀ-ն, որում տեղակայվել է մեքենայական ուսուցմամբ օժտված ՆՀՀ-ին միացված գեներատիվ-մրցակցային ցանցը: Սկզբնապես կեղծ ցանցային ենթակառուցվածքում ակտիվացված տվյալների շտեմարանը և ծառայությունները լրացվել են կեղծ ցանցային ենթակառուցվածքի օպերատորի մուտքագրած տվյալների հավաքածուներով (էնտրոպիայի մակարդակը բարձրացնելու համար): Տվյալների հավաքածուներով լցնելուց հետո կեղծ ցանցային ենթակառուցվածքի կառավարումը փոխանցվել է նեյրոնային ցանցին:

Նեյրոնային ցանցը, կեղծ ցանցային ենթակառուցվածքի կառավարումից բացի, նաև գեներացնում էր ՑԵ-ում շրջանառության տվյալներ: Տվյալները գեներացվում էին ինչպես նեյրոնային ցանցում մուտքագրված տվյալների հավաքածուների, այնպես էլ մեքենայական ուսուցմամբ օժտված ՆՀՀ-ից բխող իրադարձությունների հիման վրա, ինչը հնարավորություն էր տալիս ստեղծելու իրական ՑԵ-ի տպավորություն (յուրաքանչյուր արտաքին գրոհ ստեղծում է գեներատիվ-մրցակցային ցանցի գործարկումների եզակի, փուլաշրջանային (ցիկլիկ) շղթա՝ ցանցին ստիպելով գեներացնել տվյալների նոր հավաքածուներ): Կեղծ ցանցային ենթակառուցվածքը լրացուցիչ կերպով ստանում է տվյալների հավաքածուներ «ԱՏԻԿ»-ից *(SIEM)*, «Վազուհ» *(Wazuh)* բաց ելքային կոդով, ինչը հնարավորություն է տալիս գեներատիվ-մրցակցային ցանց մուտքագրելու նմանատիպ իրադարձությունների վերաբերյալ փոխադարձ չհամահարաբերակցող տվյալների հավաքածուներ: Առաջարկվող մոդելում բոլոր մշակվող տվյալների հավաքածուները բերված են միևնույն ձևաչափի (տվյալ դեպքում՝ *"JavaScript Object Notation",* JSON): Երևակայական միջավայրում բացազատված կեղծ ցանցային ենթակառուցվածքը ենթարկվում էր տարատեսակ գրոհների (ՏՍԱ գրոհի, համակարգչային պորտերի տեսածրման (ՀՊՏ) գրոհի, սահմանային սարք մուտք գործելու ռեկվիզիտների հատարկման գրոհի («բրուտֆորս» գրոհ), տվյալների փոխանցման հաղորդակարգերի (ՏՓՀ, *TCP, Transmission Control Protocol)* և օգտատիրոջ տվյալագրության հաղորդակարգի (ՕՏՀ, *UDP, User Datagram Protocol)* տիպի գրոհների): Միևնույն ժամանակ, ձեռնարկվել է գրոհ «ՍիՎիԻ-2022-20685» *("CVE-2022-20685")* խոցելիության կիրառմամբ, ինչի շնորհիվ հնարավոր դարձավ շրջանցել սահմանային «Սնորտ» *(Snort)* ՆՀՀ-ի պաշտպանությունը և վնասաբեր կոդը մուտքագրել ՑԵ-ի ապառազմականացված գոտում *(DMZ, Demilitarized Zone):*

Տարատեսակ գրոհների ժամանակ ճշտություն, ճշգրտություն, զգայունություն և ուրույնություն պարամետրների արժեքների տեսանելիացումը ներկայացված է 2-5-րդ նկարներում.

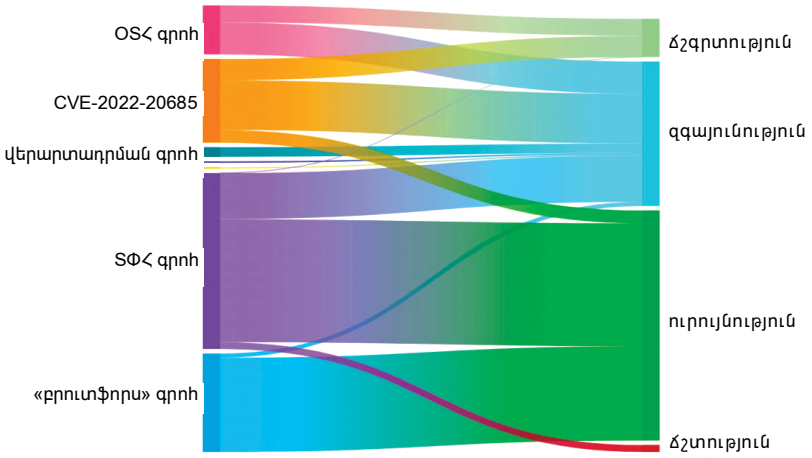


Նկ. 2. Ճշտություն, ճշգրտություն, զգայունություն և ուրույնություն պարամետրների արժեքների տեսանելիացում. ուսուցման առաջին շրջան, 2-րդ բազմակրկնություն

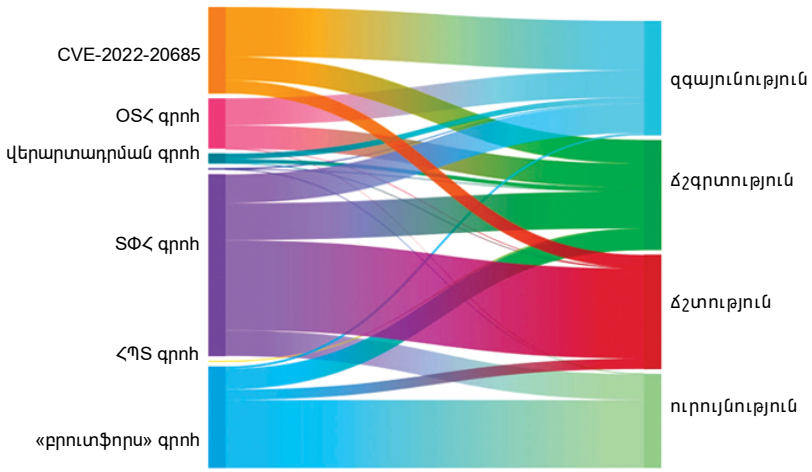


Նկ. 3. Ճշտություն, ճշգրտություն, զգայունություն և ուրույնություն պարամետրների արժեքների տեսանելիացում. ուսուցման առաջին շրջան, 4-րդ բազմակրկնություն

* Հավանական բանալիների անընդհատ որոնում:



Նկ. 4. Ճշտություն, ճշգրտություն, զգայունություն և ուրույնություն պարամետրերի արժեքների տեսանելիացում. ուսուցման երկրորդ շրջան

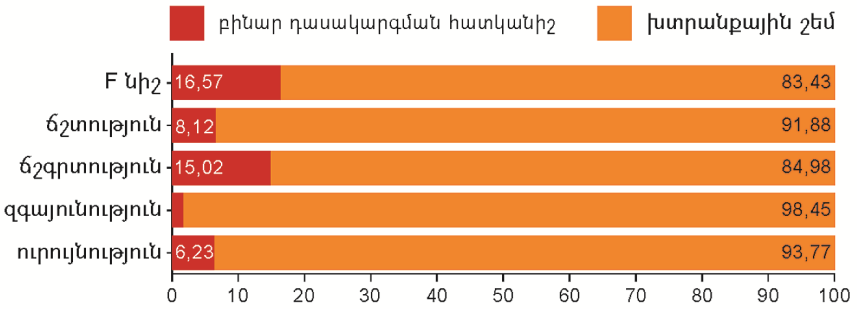


Նկ. 5. Ճշտություն, ճշգրտություն, զգայունություն և ուրույնություն պարամետրերի արժեքների տեսանելիացում. ուսուցման երրորդ շրջան

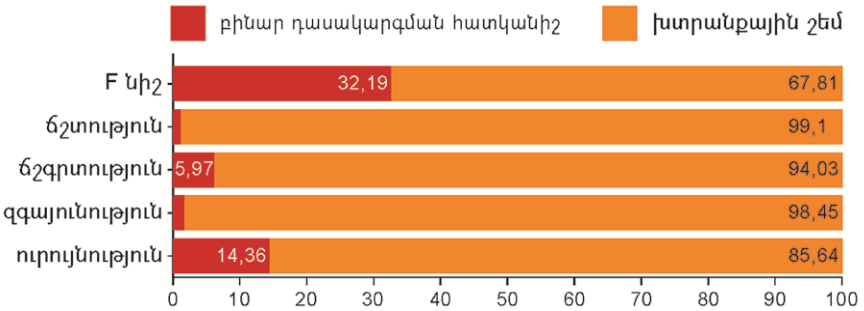
Արդյունքները

Ստացված տվյալների հիման վրա կատարվեցին ինչպես կեղծ ցանցային ենթակառուցվածքի փոփոխման վիճակագրական թեստավորումներ, այնպես էլ մեքենայական ուսուցմամբ օժտված ՆՀՀ-ի թեստավորում: Նկ. 6-10-ում ներկայացված են ուսուցման արդյունքների (%) և ուսուցման տարբեր շրջաններում մեքենայական ուսումամբ օժտված ՆՀՀ-ից ծագող իրադար-

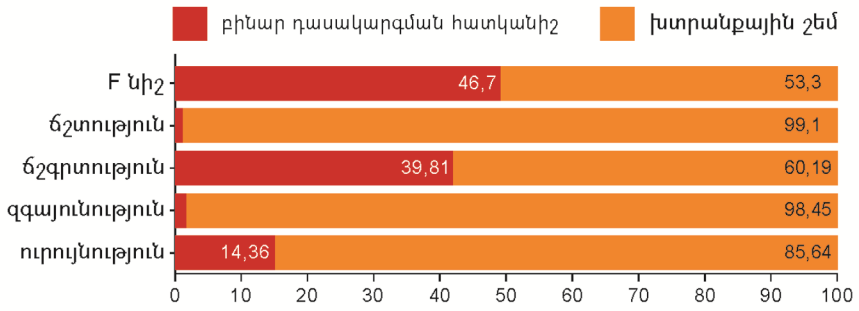
ձություններին գեներատիվ-մրցակցային ցանցի արձագանքների տեսանելիացումները:



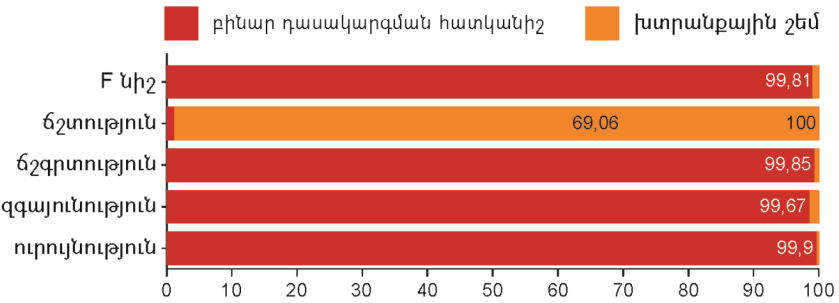
Նկ. 6. Ճշտություն, ճշգրտություն, զգայունություն, ուրույնություն պարամետրների և $F_{նիշ}$-ի արժեքների տեսանելիացում. ուսուցման առաջին շրջան



Նկ. 7. Ճշտություն, ճշգրտություն, զգայունություն, ուրույնություն պարամետրների և $F_{նիշ}$-ի արժեքների տեսանելիացում. ուսուցման երկրորդ շրջան



Նկ. 8. Ճշտություն, ճշգրտություն, զգայունություն, ուրույնություն պարամետրների և $F_{նիշ}$-ի արժեքների տեսանելիացում. ուսուցման երրորդ շրջան



Նկ. 9. Ճշտություն, ճշգրտություն, զգայունություն, ուրույնություն պարամետրերի և $F_{նիշ}$-ի արժեքների տեսանելիացում. ուսուցման չորրորդ շրջան

Գեներատիվ-մրցակցային ցանցը $F_{նիշ}$-ի օպտիմալ արժեքին հասնում է ուսուցման երրորդ շրջանում (նկ. 5, նկ. 8): $F_{նիշ}$-ի որոշումը հնարավորություն է տալիս կեղծ ցանցային ենթակառուցվածքի դասավորման ժամանակ մուտքագրվող պարամետրերի համար առաջադրելու ելքային արժեքները, որոնք նվազեցնում են նախնական հաշվարկումները: Ուսուցման 4-րդ և հաջորդ շրջաններում տեղի է ունենում գեներատիվ-մրցակցային ցանցի վերաուսուցում (նկ. 9), ինչը չարագործին հնարավորություն է տալիս միանշանակ կերպով հայտնաբերելու կեղծ ցանցային ենթակառուցվածքը: Ինքնավար համակարգի* շրջանակում ամբողջ ՑԵ-ի նմանարկման համար կատարվող կեղծ ցանցային ենթակառուցվածքները մասշտաբավորելու ժամանակ (ինչպես տեսաբանորեն, այնպես էլ ըստ սատարվող ծառայությունների) հնարավոր է ճշտություն, ճշգրտություն, զգայունություն և ուրույնություն պարամետրերի փոփոխմամբ ստեղծել ուսուցանող ընտրանքների վիճակագրորեն անկախ արժեքներ և, համապատասխանաբար, մեծացնել կեղծ ցանցային ենթակառուցվածքների նմանարկումային հաստատունությունը: Գեներատիվ-մրցակցային ցանցի ուսուցումը կատարվել է «ԹենզորՖլոու» *(TensorFlow)*, իսկ արդյունքների տեսանելիացումը՝ «ԹենզորԲորդ» *(TensorBoard)* գրադարանների կիրառմամբ:

Եզրակացություն

Հոդվածում դիտարկվել է մի մոդել, որը $F_{նիշ}$-ի նախապես որոշված արժեքի դեպքում միավորել է գեներատիվ-մրցակցային ցանցն ու կեղծ ցանցային ենթակառուցվածքը: Ստացվել են ճշտություն, ճշգրտություն, զգայունութ-

* Ինքնավար համակարգը *(Autonomous System, AS) երթուղավորման* միասնական քաղաքականություն ունեցող մեկ կամ մի քանի օպերատորի կառավարած ինտերնետային հաղորդակարգային ցանցերի (IP-ցանցեր) և երթուղավորիչների համակարգ է (տես *J. Hawkinson.* Guidelines for creation, selection, and registration of an Autonomous System (AS), Network Working Group (RFC 1930), March 1996, PP. 5–6 (https://www.rfc-editor.org/rfc/pdfrfc/rfc1930.txt.pdf)):

յուն և ուրույնություն պարամետրների այն արժեքները, որոնց դեպքում $F_{միջ}$-ն ընդունում է գեներատիվ-մրցակցային ցանցի (և համապատասխանաբար՝ կեղծ ցանցային ենթակառուցվածքի) կառավարման համար անհրաժեշտ արժեքը՝ մեծացնելով այդ ցանցի նմանարկումային հաստատունությունը: Գեներատիվ-մրցակցային ցանցի ուսուցման համար որպես մուտքային տվյալներ ծառայել են մեքենայական ուսուցմամբ օժտված ՆՀՀ-ից ստացված տվյալները[9], այն տվյալների հավաքածուները, որոնք ստացվել են[10] աղբյուրներից ստացվող տարատեսակ վնասաբեր ԾԱ-երի հիմքի վրա և «ԱՏԻԿ» *(SIEM)* համակարգից ստացված տվյալները: $F_{միջ}$-ի արժեքների և միասնական ՑԵ-ի շրջանակում գործող գեներատիվ-մրցակցային ցանցերի վերաուսուցման պահի որոշումը հնարավորություն է տալիս նաև կեղծ ցանցային ենթակառուցվածքների մասշտաբայնացման ժամանակ մեծացնելու դրանց կառավարելիությունը:

Թարգմանությունը՝ ***Թամարա Չիլինգարյանի***

ИССЛЕДОВАНИЕ МОДЕЛИ ПРИМЕНЕНИЯ НЕЙРОННОЙ СЕТИ В ЛОЖНОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЕ В СФЕРЕ ОБОРОНЫ

Т. В. ДЖАМГАРЯН, подполковник, кандидат технических наук, заместитель начальника Отдела безопасности связи и засекреченной связи Управления связи и АСУ ГШ ВС РА; Т. Н. ШАХНАЗАРЯН, генерал-майор, начальник Главного оперативного управления ГШ ВС РА – заместитель Начальника ГШ ВС РА

РЕЗЮМЕ

В статье представлены результаты расчетов и тестирования применения методов машинного обучения для управления ложной сетевой инфраструктурой. Ложной сетевой инфраструктурой и циркулирующими в ней данными управляла генеративно-состязательная сеть. В качестве параметров оценки были отобраны следующие факторы: правильность, точность, чувствительность и специфичность. Для оценки качества генеративно-состязательной сети был применен критерий минимального дискриминационного порога F_{score}.

В виртуальной среде были проведены различные виды тестирования. Было осуществлено моделирование различных атак – алгоритм генерации доменов (*DGA* атака), атака с использованием

[9] Տես *R. G. Hakobyan, T. V. Jamgharyan.* Research of Algorithm for Expanding the Database of Training Datasets of a Generative-Adversarial Network. “Bulletin of High Technology”, 2023, N 1(25) (https://doi.org/10.56243/18294898-2023.1-59):

[10] Տես “VX Vault database” (http://vxvault.net/ViriList.php); “Malware repository” (https://avcaesar.malware.lu/); “Viruses share repository” (https://virusshare.com/):

сканирования портов, атака для доступа к пограничному устройству, атака на протокол управления передачей и протокол пользовательских датаграмм типа «отказа от обслуживания» (*TCP/UDP SYN*). Управляющая ложной инфраструктурой генеративно-состязательная сеть была подключена к системе обнаружения вторжений с машинным обучением. Осуществленные теоретические расчеты и практические испытания подтверждают возможность создания ложной инфраструктуры с минимальным вмешательством со стороны оператора.

A STUDY OF A MODEL OF NEURAL NETWORK APPLICATION IN THE DECOY INFRASTRUCTURE IN THE DEFENSE SPHERE

T. V. DJAMGHARYAN, Lieutenant Colonel, PhD in Engineering, Deputy Head, Communications Security and Classified Communications Division, Signal and AMS Department, General Staff of the RA Armed Forces;
T. N. SHAHNAZARYAN, Major General, Head, Main Operative Department – Deputy Chief, General Staff of the RA Armed Forces

SUMMARY

The article discusses the results of calculations and testing of the machine learning application methods for the management of decoy infrastructure. The decoy infrastructure and the data circulating within it were managed by the generative adversarial network. The following factors were selected as estimation parameters: accuracy, precision, recall and specificity. The criterion of minimum discriminative threshold F_{score} was used to assess the quality of the generative adversarial network.

Testing of various types was conducted in the virtual environment. Various attacks were simulated – Domain Generation Algorithm (DGA attacks), port scanning attack, edge device access attack, Transmission Control Protocol attack, and User Datagram Protocol of “denial-of-service” type (TCP/UDP SYN). The generative adversarial network running the decoy infrastructure was attached to the intrusion detection system with machine learning. The theoretical calculations made and practical tests carried out come to confirm the possibility of creating the decoy infrastructure with minimum interference from the operator.