ԿԻԲԵՌՈՒԼՈՐՏՈՒՄ ՆԵՐԽՈՒԺՈՒՄՆԵՐԻ ՀԱՅՏՆԱԲԵՐՄԱՆ ՀԱՄԱԿԱՐԳԵՐՈՒՄ ՄԵՔԵՆԱՅԱԿԱՆ ՈՒՍՈՒՑՄԱՆ ԿԻՐԱՌՄԱՆ ՈՐՈՇ ԽՆԴԻՐՆԵՐԻ ՎԵՐԼՈՒԾՈՒԹՅՈՒՆ*

Թ. Վ. ՋԱՄՂԱՐՅԱՆ, փոխգնդապետ, ՀՀ ՋՈՒ-ի կապի և ԱԿՀ վարչության ավագ սպա

ՆԵՐԱԾՈՒԹՅՈՒՆ

Նոր տեխնոլոգիաների մշակումն ու ներդրումը կապված են բազմաթիվ ռիսկերի հետ: Չորրորդ արդյունաբերական (տեխնոլոգիական) հեղափոխությունն առաջացնում է և՛ հսկայական օգուտներ, և՛ մեծաթիվ մարտահրավերներ: Կարևոր է հաշվի առնել, որ աշխարհի տարածքի 17 %-ի բնակչությունը պատրաստվում է թևակոխելու երկրորդ արդյունաբերական հեղափոխության դարաշրջան, մոտ 60 %-ը (մոտ 4 միլիարդ մարդ) սպասում է երրորդ արդյունաբերական հեղափոխության փուլին, և աշխարհի միայն մի փոքր մասն է արդեն անցել «Արդյունաբերություն 4.0»-ի փուլը[1]: Զարգացման այս անհամաչափության աճումը կհանգեցնի նոր զինված հակամարտությունների, և տեխնոլոգիական զարգացման ավելի ցածր մակարդակում գտնվող պետությունները կհակամարտեն ավելի բարձր մակարդակում գտնվողների հետ: Չորրորդ արդյունաբերական հեղափոխության ցուցիչներից մեկը, ըստ Կ. Շվաբի, «թվային բլոկն» է, որը կամուրջ է ֆիզիկական և թվային իրականությունների միջև[2]: Չորրորդ արդյունաբերական հեղափոխությունն առանձնահատուկ ազդեցություն է գործում կառավարման գործիքների վրա, քանի որ նկատվում է ակտիվ անցում կենտրոնացված կառավարումից դեպի ապակենտրոնացված կառավարում: Համապատասխանաբար կաճի նաև ցանցային ենթակառուցվածքի վրա հարձակումների (ներխուժումների) թիվը:

Ցանցային ենթակառուցվածքի վրա հարձակումների աճումը և զինված հակամարտությունների փոխադրումը տեղեկատվական տարածություն կհանգեցնեն այն բանին, որ զինված ուժերը «դասական» պատերազմների վարումից կանցնեն ցանցակենտրոն մոդելով ծավալվող պատերազմների վարմանը**: Որպես արդյունք՝ արդեն այսօր սկսել են աճել հարձակումների

---

* Հոդվածն ստացվել է 11.01.2023: Հոդվածի գրախոսությունը ստացվել է 11.04.2023:

[1] Տես *Կ. Շվաբ.* Четвертая промышленная революция. «World Economic Forum», 2016:

[2] Տես նույն տեղում:

** Ցանցակենտրոն պատերազմը (*Network-Centric Warfare*, կամ *Network-Centric Operations, NCW,* կամ *NCO)* պատերազմի վարման (ուժերի կառավարման) մոդել է, որը խարսխվում է նորագույն տեղեկատվական տեխնոլոգիաների, համակարգչային և զգայա-

թիրախ դարձած ցանցային ենթակառուցվածքին ներկայացվող պահանջները: Այս համատեքստում ուշադրության են արժանի ցանցակենտրոն պատերազմի կազմակերպման հատկապես հետևյալ կանոնները (դրույթները).

- *հուսալիորեն գործող ցանցերով միավորման դեպքում ուժերն ստանում են տեղեկույթի փոխանակումը բարելավելու հնարավորություն,*
- *տեղեկույթի փոխանակումը բարձրացնում է տեղեկույթի որակը և ընդհանուր իրավիճակային իրազեկվածության աստիճանը,*
- *ընդհանուր իրավիճակային իրազեկությունը ապահովում է համագործակցությունը և ինքնահարաբերակցումը (self-synchronization), բարձրացնում հրամանատարության կայունությունն ու արագությունը:*

Որպես մարտական գործողությունների մոդել՝ լայնորեն կիրառվում է «ղեկավարման փուլ» հասկացությունը, կամ այսպես կոչված ԴԿՈՋ օղակը (Դիտում *(Observation)* – Կողմնորոշում *(Orientation)* – Որոշում *(Decision)* – Ջեռնարկում *(Action),* OODA)[3]: Իսկ ճիշտ որոշումների կայացման համար անհրաժեշտ է, որ որոշում կայացնող անձը[*] *(decision maker)* լիարժեք կերպով տիրապետի *իրավիճակային տեղեկույթին, այսինքն՝ լինի իրավիճակայնորեն իրազեկված*[**]:

Ըստ այդմ՝ պարզ է դառնում, որ ցանցակենտրոն պատերազմի դեպքում ցանցային ենթակառուցվածքի կայունությունը եթե ոչ գերակա, ապա առնվազն շատ կարևոր դեր կունենա:

Այսօր տեղեկատվական անվտանգության ոլորտի տարբեր հետազոտողներ ակտիվորեն ուսումնասիրում են ցանցային ենթակառուցվածքի տեղեկատվական անվտանգության ապահովման խնդիրը տարբեր *սպառնալիքների մոդելների* ամբողջ սպեկտրով՝ մասնավորապես կիրառելով Փարկերի վեցորդության (հեքսադի), ԳԱՄ-ի (գաղտնիություն, ամբողջականություն, մատչելիություն, կամ *CIA (confidentiality, integrity, availability))* և

րարական տեխնիկայի կիրառմամբ ստեղծված մեկ տեղեկատվական ցանցում ռազմական գործողությունների բոլոր մասնակիցների (հրամանատարություն, ՍՈՏ, կենդանի ուժ և այլն) միավորման գաղափարի վրա (տես, օրինակ, “Network Centric Operations: Background and Oversight Issues for Congress”. CRS Report for Congress. Updated 15 March 2007 (https://sgpfas.org/crs/natsec/RL32411.pdf); “Disruption Tolerant Mobile Wireless Networks”. “mesh dynamics” (https://www.meshdynamics.com/military-mesh-networks.html); *Է. Կ. Սարկիսյան, Ա. Ջ. Պետրոսյան,* Ցանցակենտրոն պատերազմը որպես նոր ձևի կազմակերպվածք և կառավարման նոր համակարգ: «ՀԲ», 2022, հմ. 1):

[3] Տես *В. И. Ковалев, Г. Г. Малецкий, Ю. А. Матвиенко.* Концепция «сетецентрической» войны для армии России: «множитель силы» или ментальная ловушка?». «Экономические стратегии», 2013, № 5 (https://spkurdyumov.ru/networks/koncepciya-sete centri cheskoj-vojny/2/); *Գ. Վ. Տավարածյան,* Մարտական գործողությունների տեղափոխում հակառակորդի տարածք. ռազմավարական դիտարկում: «ՀԲ», 2019, հմ. 1:

[*] Որոշում կայացնող անձ *(decision maker)*՝ որոշումների կայացման տեսության մեջ, որոշման սուբյեկտ, որն օժտված է որոշակի լիազորություններով և պատասխանատու է կայացված և իրագործված կառավարային որոշման հետևանքների համար:

[**] Իրավիճակային իրազեկվածություն՝ աշխատանքային միջավայրի վիճակի իմացություն:

Դոլև-Յաոյի մոդելները[4]: Ցանցային ենթակառուցվածքի անվտանգության ճարտարապետության համար առանցքային են մի քանի բաղադրիչներ, որոնցից հարկ ենք համարում նշել կիրառվող բազմաթիվ անվտանգային քաղաքականությունները, «սպառնալիքների մոդելը» և ցանցային ենթակառուցվածքի անվտանգությունն ապահովող սարքավորանքի փոխդասավորությունների կանոնները: Ցանցային ենթակառուցվածքի պաշտպանությունը պետք է լինի բազմամակարդակ և փոխլրացնող (կոմպլեմենտար): Ցանցային ենթակառուցվածքների անվտանգության հետազոտման առանձին խնդիրներ են կայուն վիճակից ենթակառուցվածքի դուրսբերման և դրա ապակայունացման չափանիշների սահմանումը[5]:

Ցանցային ենթակառուցվածքին ներկայացվող պահանջներից մեկը *կայունությունն* է: Այն կարևոր է ինչպես «ֆիզիկական», այնպես էլ ծրագրայնորեն որոշվող (ծրագրայնորեն փոխդասավորվող) ցանցերի (ԾՈՑ) *(Software Defined Networking, SDN)* դեպքում, քանի որ տարբեր տեսակների (հաշվարկային, փոխադրական (տրանսպորտային), հեռահաղորդակցային) ցանցերի աճող զուգամիտումը ցույց է տալիս, որ տարբեր բաղադրիչների և ծառայությունների փոխանցումը ԾՈՑ-ին ենթակառուցվածքի անվտանգության համար ստեղծում է նոր սպառնալիքներ:

Ցանցային ենթակառուցվածքի դեմ ուղղված տարաբնույթ սպառնալիքները չեզոքացնելու համար օգտագործվում են ապարատածրագրային լուծումներ՝ հիմնված տարբեր սկզբունքների և գործունեության ալգորիթմների վրա:

Ցանցային ենթակառուցվածքի անվտանգության ճարտարապետության կարևոր տարրերից է ներխուժումների հայտնաբերման համակարգը (ՆՀՀ, *Intrusion Detection System, IDS):* Նման համակարգերի օգտագործման հնարավորություններն առավել լիարժեք կերպով պատկերացնելու համար կարևորություն է ստանում այն ցանցային խնդիրների խմբավորման ու որոշարկման հարցը, որոնք ներխուժումների հայտնաբերման համակարգերի օգտագործման տեսակետից ծառանում են ցանցային անվտանգության հետազոտողների առջև:

ՈՐՈՇ ՑԱՆՑԱՅԻՆ ԽՆԴԻՐՆԵՐԻ ԽՄԲԱՎՈՐՄԱՆ ԵՎ ՍԱՀՄԱՆՄԱՆ ՀԱՐՑԸ

Սույն հետազոտությունում ձևակերպված են այն հիմնական խնդիրները, որոնց բախվում են իրենց կազմում մեքենայական ուսուցմամբ (ՄՈՒ) օժտված ՆՀՀ-ներ ունեցող ցանցային ենթակառուցվածքների անվտանգության հետազոտողները:

[4] Տես *G. Stoneburner.* Underlying Technical Models for Information Technology Security. NIST Special Publication 800-33, 2001 (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-33.pdf):

[5] Տես *T. V. Jamgharyan, V. H. Ispiryan.* Network Infrastructures Assessment Stability. Proceedings of 13th International Conference on Computer Science and Information Technologies (CSIT). Yerevan, Armenia, 2021, PP. 199–203:

Ցանցային ենթակառուցվածքը շահագործելու դեպքում կարևոր խնդիրներից մեկը ՆՀՀ և (կամ) դրա հատվածների վրա հարձակումների չեզոքացման խնդիրն է: ՆՀՀ-ն ոչ միայն գործում է ատոմական փաթեթներով, այլև հնարավորություն է տալիս կատարելու փոխանցուղու *(traffic)* փաթեթի կառուցվածքային վերլուծություն: Բացի այդ, ՆՀՀ-ները հնարավորություն են տալիս առանձնացնելու ցանցերի պարագծերը և չեզոքացնելու ցանցային ենթակառուցվածքի դեմ ուղղված բազմաթիվ տարաբնույթ սպառնալիքներ, որոնք իրագործվում են վնասաբեր ծրագրային ապահովման միջոցով: Կիբեռհարձակումների թվի և տեսակների աճմանը զուգընթաց (ինչպես առանձին չարագործների, այնպես էլ կազմակերպված խմբերի դեպքում) հրատապ ու կարևոր է դառնում ցանցային ենթակառուցվածքի բոլոր երեք մակարդակներում (հիմնական, բաշխման, հասանելիության *(core, distribution, access))* հնարավոր հարձակման չեզոքացման խնդիրը[6]: Տարբեր ՆՀՀ-ներ բարդ ապարատածրագրային համալիրներ են (օրինակ՝ Սնորտ (*Snort), Սուրիկաուա (Suricata), Զիկ (Zeek)* ծրագրային ապահովում, տարբեր ՆՋՖՎ-ներ *(Next-Generation Firewall, NGFW)*, ՈՒԹՄ (*Unified Thread Management, UTM)* ապարատածրագրային համալիրներ): Բացի այդ, նախագծողները դասակարգման ժամանակ առանձնացնում են այն սարքերը, որոնք կարող են արձագանքել կոնկրետ տեսակի սպառնալիքներին: Գոյություն ունեցող ՆՀՀ-ները հիմնականում գործում են ՕՍԻ *(Open Systems Interconnection, OSI)* մոդելի 3–7 մակարդակներում և ՍԻԵՄ *(Security Information and Event Management, SIEM)* համակարգերի հետ համատեղ, քանի որ դրանք չարագործությունների համար հզոր խոչընդոտ են: Ենթակառուցվածքի ավտոմատացման աստիճանի մեծացումը և մեքենա–մեքենա (ՄՄ, *Machine-to-Machine*) փոխազդեցության աճումը փոխել են ցանցային ենթակառուցվածքի վրա հարձակումների համար օգտագործվող գործիքակազմը: Այս առումով ցանցային և ենթակառուցվածքային անվտանգության ապահովման հետազոտությամբ զբաղվողները ձևակերպել են մի խնդիր, որը միավորել է գոյություն ունեցող գրեթե բոլոր «դասական» տեսակների ՆՀՀ-ները[7]: Մասնավորապես՝ պարզվել է, որ եղած «դասական» ՆՀՀ-ներն

[6] Տես *Chris Carthern, William Wilson, Noel Rivera.* Cisco Networks. Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA, 2nd Edition, 2021; նաև՝ *Omar Santos, John Stuppi.* CCNA Security 210-260 Official Cert Guide. Cisco Press. Indianapolis, 2015:

[7] Տես *О. Шелухин, Д. Сакалема, А. Филинова.* Обнаружение вторжений в компьютерные сети. М., 2018; *Shisrut Rawat et al.* Intrusion detection systems using classical machine learning techniques versus integrated unsupervised feature learning and deep neural network, 01.10.2019 (https://arxiv.org/abs/1910.01114); *R. Atefinia, M. Ahmadi.* Performance Evaluation of Apache Spark MLib Algorithms on an Intrusion Detection Dataset. "Journal of Computing and Security". Isfahan University, Iran, 2022, Vol. 9, N 1 (https://arxiv.org/abs/2212.05269); *А. Браницкий, И. Котенко.* Анализ и классификация методов обнаружения сетевых атак. «Труды СПИИРАН», 2016, вып. 45, сс. 207–244; *C. Chio, D. Freeman.* Machine Learning and Security: Protecting Systems with Data and Algorithms, 2020:

աշխատում են գործողության կանոնների և ալգորիթմների նկարագրված հավաքածուների շրջանակներում և ի վիճակի են հայտնաբերելու միայն այն սպառնալիքները (հարձակումներ, խոցելիություն, ցանցային անկանոնություններ, չարագործ ծրագրային ապահովման բաղադրիչներ), որոնց համար կա համապատասխան հայտնաբերիչ (դետեկտոր): Այլ կերպ ասած՝ «դասական» ՆՀՀ-ներն իրենց որոշարկվածության պատճառով չեն կարողանում հայտնաբերել այն հարձակումները, որոնք չեն ներառվում սիգնատուրային տվյալների շտեմարանի հիմքում դրված կանոնների շրջանակում: Տվյալ դժվարությունը հաղթահարելու նպատակով սահմանափակ որոշարկային ՆՀՀ-ի համար առաջարկվել է ՆՀՀ զգայարարի «տեսադաշտ» հասկացությունը[8]: Էվրիստիկական ալգորիթմների հիման վրա աշխատող ՆՀՀ-ները նույնպես սահմանափակ են վնասաբեր ծրագրերի հայտնաբերման գործում, քանի որ այդ ալգորիթմները տարբեր մեթոդների կիրառմամբ ձևավորված ալգորիթմների բարդ կազմություն (կոմպոզիցիա) են:

Մեքենայական ուսուցման (ՄՈՒ, *Machine Learning, ML)* մեթոդների օգտագործումն է՛լ ավելի է սրում պրոբլեմը, քանի որ ՄՄ–ՄՈՒ *(M2M&ML)* կապակցությունն ի վիճակի է ապակայունացնելու ցանցային ենթակառուցվածքը (կամ դրա հատվածը): Պարզ է, որ որպես հարձակման գործիք ՄՈՒ-ն կիրառող չարագործների հարձակումներին հաջողությամբ կարող է դիմակայել միայն նմանատիպ (ՄՈՒ-ի հիման վրա գործող) համակարգը: Որպեսզի ստեղծվի մեքենայական ուսուցմամբ օժտված կամ լիովին դրա վրա հիմնված ՆՀՀ, «դասական» ՆՀՀ որոշարկվածության պրոբլեմը տրոհվել է մի շարք խնդիրների:

Ցանցային անվտանգության հետազոտությամբ զբաղվող մասնագետները մշտապես կատարելագործում են մեքենայական ուսուցման միջոցով վնասաբեր հարձակումներին հակազդեցության մեթոդների գիտական զինանոցը: Սույն աշխատության մեջ դիտարկվում են հետազոտողների ձևակերպած որոշ խնդիրներ՝ ներխուժումների հայտնաբերման համակարգում մեքենայական ուսուցման մեթոդները կիրառելու պարագայում:

Հիմնական խնդիրներ են.

- ցանցային ենթակառուցվածքի վրա հաջող հարձակման հավանականության հաշվարկում, երբ հարձակվողն օգտագործում է մեքենայական ուսուցման գործիքարանը[9],
- տեղեկութային անվտանգության միևնույն միջադեպին (անցանկալի կամ անսպասելի իրադարձությանը) տարբեր զգայարարների արձագանք-

[8] Տես *Օ. Շելուխին, Դ. Սակալեմա, Ա. Ֆիլինովա,* Նշ. աշխ.: Զգայարարի (տվիչի) «տեսադաշտն» այն փոխանցուղին է, որը կարող է գրանցել զգայարարը:

[9] Տես *T. V. Jamgharyan, V. H. Ispiryan.* Model of Generative Network Attack. Proceedings of 13th International Conference on Computer Science and Information Technologies (CSIT). Yerevan, Armenia, 2021, PP. 90–94:

ման (հայտնաբերման) հետևանքով դրանց ԻԴ – ԿԴ – ԻԲ – ԿԲ* գործարկումների որոշում[10],

- նեյրոնային ցանցերի կիրառմամբ կառուցված զգայարարների «տեսադաշտի» ընդլայնում և փոփոխակային վերակառուցում[11],
- պարփակված փոխանցուղու վարքային վերլուծություն,
- համակարգում չնկարագրված փոխանցուղու հայտնվելու դեպքում այդ համակարգի վարքի նկարագրություն,
- մեքենայական ուսուցման համակարգերի անվտանգության ապահովում. ՄՈՒ-ի կիրառմամբ կառուցված ՆՀՀ-ները հավանականային համակարգեր են, և դրանց ելքային արդյունքների արժանահավատությունը պայմանավորված է նաև ԻԴ և ԿԴ գործարկումներին դրանց դիմակայելու մակարդակով[12],
- ՄՄ և ՄՈՒ-ի կիրառմամբ ձեռնարկված հարձակումների ժամանակ վնասաբեր ծրագրերի դասակարգման առանձնահատկությունների տարբերակում[13],
- «անվտանգության» գերհամակարգում ՄՈՒ-ի կիրառմամբ ներխուժումների հայտնաբերման համակարգի առկայության կետերի որոշում,
- ՄՈՒ-ով ՆՀՀ-ների ուսուցման համար **որակյալ** տվյալների հավաքածուների ստեղծում (գեներացում): Հետազոտողներն օգտագործում են վնասաբեր ծրագրերի գոյություն ունեցող հանրային շտեմարաններ[14], սակայն համապատասխան տվյալների շտեմարանների ադմինիստրատորները հանրահասանելի են դարձնում այն վնասաբեր ծրագրերը, որոնք կորցնում են իրենց արդիականությունը հանրային հասանելիության պահին,
- նեյրոնային ցանցի ուսուցման համար ծանոթագրված** տվյալների

---

* Իրական դրական՝ *true positive, TP,* կեղծ դրական՝ *false positive, FP*, իրական բացասական՝ *true negative, TN,* կեղծ բացասական՝ *false negative* , *FN:*

[10] Տես *S. Das.* FGAN: Federated Generative Adversarial Networks for Anomaly Detection in Network Traffic. BITS Pilani, Rajasthan, India, 22 March 2022:

[11] Տես *Lening Li, Haoxiang Ma, Shuo Han, Jie Fu.* Synthesis of Proactive Sensor Placement In Probabilistic Attack Graphs (https://arxiv.org/abs/2210.07385):

[12] Տես *K. Jallad, M. Aljnidi, M. Desoki.* Big data analysis and distributed deep learning for next-generation intrusion detection system optimization, 28.09.2022 (https://arxiv.org/abs/ 2209.13961):

[13] Տես *S. Ackerman, O. Raz, M. Zalmanovich, A. Zlotnick.* Automatically detecting data drift in machine learning classifiers, 10.11.2021 (https://arxiv.org/abs/2111. 05672):

[14] Տես “MalwareBazaar Database” (https://bazaar.abuse.ch/browse/); “Malware-database” (http://vxvault.net/ViriList.php); “Malware repository” (https://avcaesar. malware.lu/); “Viruses repository” (https://virusshare.com/); «Программное обеспечение mimikatz» (https://github. com/search?q=mimikatz); «Интернет-ресурс проверки вредоносных файлов» (https://www.virustotal.com):

** Ծանոթագրումը՝ չմշակված տվյալների պիտակավորումն է, որով նշված տվյալների հավաքածուն դառնում է մեքենայական ուսուցման համար կիրառելի:

ստացում. մեքենայական ուսուցման ՆՀՀ-ներն այս փուլում ի վիճակի չեն հայտնաբերելու վնասաբեր ծրագրերը՝ առանց համապատասխան տվյալների հավաքածուներով «ուսուցանվելու»: Մեքենայական ուսուցման ՆՀՀ-ն մեծ թվով սխալներ կառաջացնի, եթե ուսուցման համար օգտագործվեն ոչ ծանոթագրված և «աղմկոտ» տվյալներ: Հատկապես կարևոր է ունենալ վավերացման տվյալների հավաքածու, որը չի պարունակում «աղմուկներ» կամ դրանց թիվը կրճատվում է մինչև նվազագույն թույլատրելի արժեքը[15],

- մեքենայական ուսուցման հիման վրա կառուցված ՆՀՀ-ների ուսուցման արագության մեծացում (եթե տվյալների որևէ շտեմարանում չներառված վնասաբեր ծրագիրն ունի տվյալների այնպիսի բաշխում, որը տարբերվում է նախնական ուսումնական նմուշների բաշխումից, ապա նոր վնասաբեր ծրագրերի հանդիպելու դեպքում հայտնաբերման մոդելի արդյունավետությունը կնվազի),
- հարձակման ժամանակ ՄՈՒ-ի օգտագործմամբ սպառնալիքի աստիճանի ճիշտ հաշվարկում (մեքենայական ուսուցման վրա հիմնված ՆՀՀ մշակելիս անհրաժեշտ է ճիշտ հաշվարկել ցանցային ենթակառուցվածքը վտանգող սպառնալիքի աստիճանը):

ՆՀՀ-ում ՄՈՒ-ի օգտագործման մասնավոր խնդիրների շարքում կարելի է ներառել՝

- կառավարման կարգավորման* վրա հիմնված հայտնաբերման խնդիրները,
- ոչ ճշգրիտ հեշի** վրա հիմնված աղոտարկված (օբֆուսկացված *obfuscated)* ծրագրային ապահովման ուսումնասիրության խնդիրները[16]: Գոյություն ունեցող ՆՀՀ-ների համար մշակվել է «սսդիպ» (“*ssdeep”*) ծրագրային ապահովումը, սակայն դրա արդյունավետությունը նվազում է, երբ չարագործները օգտագործում են ՄՈՒ-ն,

[15] Տես *Т. В. Джамгарян.* Исследование алгоритма подготовки данных для обучения генеративно-состязательной сети. «Известия Высоких технологий», 2022, №1(19):

* Կառավարման կարգավորում *(Inversion of Control, IoC.).* այն արտեֆակտների բազմությունը, որոնց հիման վրա հնարավոր է հայտնաբերել վնասաբեր ծրագրերը՝ ռեեստրի ճյուղեր, բեռնվող գրադարաններ, *IP* հասցեներ, բայթերի հաջորդականությունը՝ ծրագրաշարի տարբերակներ, ամսաթիվ և ժամային գործարկումներ, ներգրավված պորտեր, ռեսուրսի համապիտանի ցուցիչներ *(URL)* և այլն:

** Հեշ (անգլ. *hash*)՝ 1. մանր կտրտած միս, աղացած միս, 2. խճճանք, 3. խճողակ. խորհրդանիշների ունիկալ հավաքածու, որն ստացվել է ցանկացած ծավալով մուտք գործող տեղեկույթի փոխակերպմամբ և հատուկ է միայն տեղեկույթի այդ զանգվածին:

[16] Տես *T. Jamgharyan.* Research of Obfuscated Malware with a Capsule Neural Network. “Mathematical Problems of Computer Science”, 2022, N 58; նաև՝ *Tuan-Hong Chua, Iftektar Salam.* Evaluation of machine learning algorithms in network-based intrusion detection system (https://arxiv.org/pdf/2203.05232.pdf):

❖ բազմաձև (պոլիմորֆ) և կերպափոխային (մետամորֆ) վնասաբեր ծրագրային կոդը մեքենայական ուսուցման միջոցով հայտնաբերելու խնդիրը:

Ենթակառուցվածքի անվտանգության կարևոր խնդիր է ՆՀՀ գործառության և մշակված տվյալների արժանահավատության* ապահովումը[17]:

ՄՈՒ-ով ՆՀՀ-ն աշխատում է որոշակի ապարատային ապահովմամբ և օգտագործում է դրա ռեսուրսը, ինչը հետազոտողների համար ստեղծում է նոր խնդիրներ:

Հատուկ հետազոտությամբ ուսումնասիրվել են տվյալ ժամանակաշրջանում ներխուժումների հայտնաբերման համակարգերի զարգացումն ու տաքսոնոմիան[18]: Մասնավորապես՝ նկարագրված և մի շարք այլ խնդիրներով որոշվում են ներխուժումների հայտնաբերման համակարգերում մեքենայական ուսուցման կիրառման հետազոտության վեկտորները: Դրանցից մի քանիսը կարելի է ձևակերպել հետևյալ կերպ.

- կատարողականության ցուցանիշների ստեղծման խնդիր,
- «կատարողականության մոդելի»* կառուցման խնդիր,
- «կատարողականության բազմաչափ տարածության» կառուցման խնդիր,
- հետազոտվող տվյալների հավաքածուների չափերի նվազեցման խնդիր,
- կատարողականության չափման կրկնելիության խնդիր, որը համարվում է առավել դժվարություններից մեկը, քանի որ մեքենայական ուսուցմամբ ՆՀՀ-ների դեպքում այս դժվարությունը պայմանավորված է հենց մեքենայական ուսուցման հավանականային բնույթով,
- կատարողականության թեստավորումը կատարող նեյրոնային ցանցի (ծրագրային ապահովման) աշխատանքի մշտազննման խնդիր,
- ՄՈՒ-ով ՆՀՀ պարամետրերի չափման ժամանակ «դիտորդի էֆեկտի»** (չափման ազդեցության) նվազարկման խնդիր,
- մի քանի նեյրոնային ցանցեր օգտագործելու դեպքում «բաշխված կատարողականությունը» չափելու խնդիր[19]:

---

[17] Տես «Качество служебной информации». Национальный стандарт Российской Федерации, ГОСТ Р 51170–98. М., 2020: Տվյալների արժանահավատությունը մշակվող տվյալների՝ թաքնված սխալներ չունենալու հատկությունն է:

[18] Տես *Tarfa Hamed, Jason B. Ernst, Stefan C. Kremer.* A Survey and Taxonomy of Classifiers of Intrusion Detection Systems. “Computer and Network Security Essentials”, 2017, PP. 21–39:

* Կատարողականության մոդելը ներառում է բոլոր այն գործոնները, որոնք կարևոր են կատարման համար՝ ելակետային կոդ, կատարման միջավայր, մուտքային տվյալներ և կատարողականի բաշխում:

** «Դիտորդի էֆեկտը» դիտարկման գործընթացի ազդեցությունն է արդյունքի վրա:

[19] Տես *A. Akinshin.* Pro. NET Benchmarking. The Art of Performance Measurement, 1st Edition. Apress, 2019:

Զարգացման միտումները ցույց են տալիս, որ շարժական ու ներկառուցված համակարգերի թվի աճման հետ մեծանում է ցանցային ենթակառուցվածքի վրա «հարձակման մակերեսը», և մշակվող տվյալների պաշտպանությունը հնարավոր է միայն մեքենայական ուսուցմամբ ներխուժումների հայտնաբերման համակարգերի կիրառման դեպքում:

Մեր կատարած հետազոտություններից մեկի արդյունքներով՝ առաջարկել ենք աղոտարկված վնասաբեր ծրագրային ապահովումը հայտնաբերելու համար կիրառել համատեքստով գործարկված կտորավոր հեշավորման (ՀԳԿՀ) մեթոդը[*] *(context triggered piecewise hashing method)* կապսուլային նեյրոնային ցանցի օգտագործմամբ[20]: Հետազոտության արդյունքների հրապարակումից հետո (2022 թ. նոյեմբերի 25) կատարվել է ծրագրային ապահովման որոշակի բարելավում *(հետազոտության հետագա դինամիկան արտացոլված է* «Գիտհաբ» *(“GitHub”) շտեմարանում*[21]): Մասնավորապես՝ փոխվել են նեյրոնային ցանցի «կշիռների» ակտիվացման արժեքները և ավելացվել են կապսուլային նեյրոնային ցանցի երկու նոր շերտեր, ինչը հնարավորություն է տալիս մեծացնելու «սոֆտմաքս» (“*softmax*”) ֆունկցիայի[**] արժեքը «կշիռների» ակտիվացման ավելի փոքր արժեքներով: Ընդսմին մուտքային տվյալների հավաքածուների գործնականորեն նշանակալի նվազագույն արժեքը համատեքստամասնատված հեշավորման մեթոդի կիրառման շնորհիվ կրճատվել է մինչև 15 բայթ:

Այս բոլոր փոփոխությունների միջոցով բարելավվել է աղոտարկված վնասաբեր ծրագրերի հայտնաբերման ճշգրտությունը 0,46÷0,48 %-ով համապատասխան տվյալների հավաքածուների (կամ դրանց հատվածների) առկայության դեպքում:

Տարբեր «ուսուցման դարաշրջաններում»[***] կապսուլային նեյրոնային ցանցի կիրառմամբ «միմիկաց» *(“mimikatz”),* «աթենա» *(“athena”),* «էնգրատ» *(“engrat”),* «գրամ» *(“grum”),* «սուրտր» (“*surtr”),* «դայր» *(“dyre”)* աղոտարկված վնասաբեր ծրագրային ապահովումների հայտնաբերման և դասակարգման արդյունքները գրաֆիկական եղանակով ներկայացված են նկ. ա–դ-ում:

---

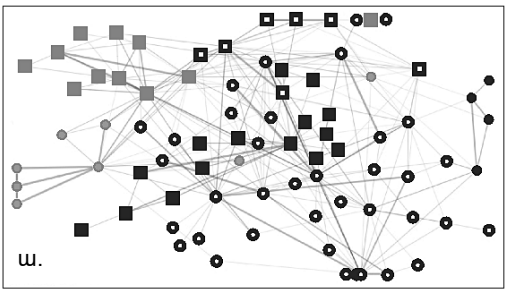
[*] Տես *Tom Wilson.* Context Triggered Piecewise Hashing to Detect Malware Similarity. «Nettitude labs», 30 June 2015 (https://labs.nettitude.com/blog/context-triggered-piecewise-hashing-to-detect-malware-similarity/)):

[20] Տես *T. Jamgharyan.* Research of Obfuscated Malware with a Capsule Neural Network:

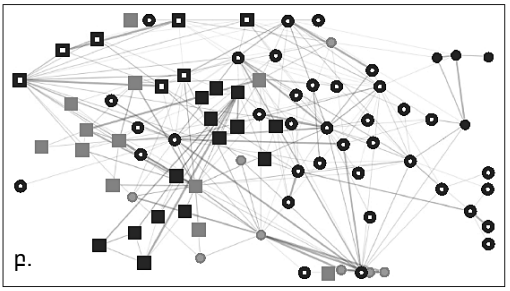
[21] Տես “Popular repositories” (https://github.com/T-JN):

[**] «Սոֆտմաքսը» մի ֆունկցիա է, որը լոգիտները (թվերի բազմությունները) վերածում է հավանականությունների, որոնց գումարը հավասար է մեկի (տես *Yan Goodfellow, Yoshua Bengio, Aaron Courville.* Deep Learning, 2020 (www.deeplearningbook.org)):

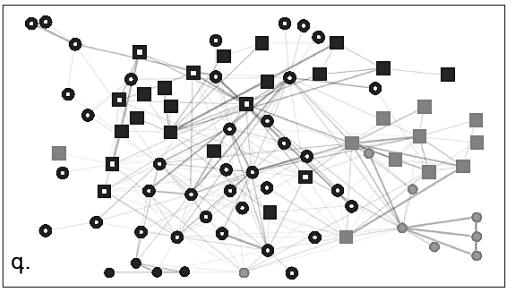
[***] «Ուսուցման դարաշրջան» (Эпоха обучения). ուսուցման բազմակրկնական (իտերատիվ) ժամանակաշրջան:



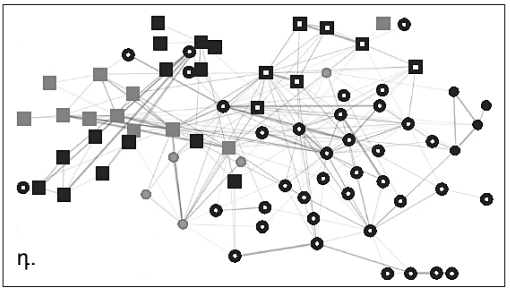
ա. Ոխուցման 1-ին դարաշրջան
(ՀԳԿՀ 15 բայթ արժեքի դեպքում)



բ. Ոխուցման 2-րդ դարաշրջան
(ՀԳԿՀ 15 բայթ արժեքի դեպքում)



գ. Ոխուցման 3-րդ դարաշրջան
(ՀԳԿՀ 20 բայթ արժեքի դեպքում)



դ. Ոխուցման 4-րդ դարաշրջան
(ՀԳԿՀ 15 բայթ արժեքի դեպքում)

Նկ. ա–դ. Դասակարգված վնասաբեր ծրագրային ապահովման տեսանելիացում

Պայմանական նշաններ

- «միմիկաց»
- «դայր»
- «գրամ»
- «աթենա»
- «էնգրատ»
- «սուրտր»

ՏԵՍԱՆԵԼԻԱՑՎԱԾ ԱՐԴՅՈՒՆՔՆԵՐԻ ՄԵԿՆԱԲԱՆՈՒԹՅՈՒՆ

Ինչպես երևում է նկարից, ՀԳԿՀ արժեքի նվազումը հնարավորություն է տալիս ավելի մանրակրկիտ լուծելու ցանցային փոխադրման ընդհանուր հոսքում վերը նշված վնասաբեր ծրագրերի դասակարգման խնդիրը: «Սոֆտմաքս» ֆունկցիայի բարելավմամբ նեյրոնային ցանցի կշիռների փոփոխությունը հնարավորություն է տվել, բացի դասակարգման խնդիրը լուծելուց, 4,3-5 %-ով բարելավելու տարբեր տեսակի վնասաբեր ծրագրերի միջև կապերի հայտնաբերման արդյունքները: Մասնավորապես՝ հնարավորություն է ստեղծվել նախագծված ՄՈՒ-ով ՆՀՀ-ի միջոցով նաև հայտնաբերելու վերը նշված վնասաբեր ծրագրերում հաշվեկարգային գործընթացները և գրադարանային ծրագրերը: ՀԳԿՀ արժեքի նվազմամբ և «սոֆտմաքսի» արժեքի միաժամանակյա բարձրացմամբ հնարավոր է դարձել հայտնաբերել աղոտարկված «սուրտր», «դայր», «միմիկաց», «աթենա», «էնգրատ», «գրամ» ծրագրային ապահովումը՝ առանց հայտնաբերման և դասակարգման օրինաչափությունը խեղաթյուրելու, ինչի շնորհիվ բարելավվում է աղոտարկված ծրագրային ապահովման հայտնաբերման ճշգրտությունը:

ԱՄՓՈՓՈՒՄ

Այսպիսով՝ չորրորդ արդյունաբերական հեղափոխության ցուցիչներից մեկը «թվային բլոկն» է, որը կամուրջ է ֆիզիկական և թվային իրականությունների միջև: Ամբողջ թվային իրականությունը տվյալների ցանցերի միջոցով միավորված սարքերի շարք է: Ըստ այդմ՝ տվյալ աշխատության մեջ ուսումնասիրվել են ցանցային ենթակառուցվածքի դեմ ուղղված սպառնալիքները, հատկապես՝ ցանցակենտրոն պատերազմի որոշ առանձնահատկությունների հաշվառմամբ:

Ցանցային ենթակառուցվածքի դեմ ուղղված տարաբնույթ սպառնալիքները չեզոքացնելու համար օգտագործվում են ապարատածրագրային լուծումներ՝ հիմնված տարբեր սկզբունքների և գործունեության ալգորիթմների վրա:

Ցուցակագրվել են ներխուժումների հայտնաբերման՝ մեքենայական ուսուցման կիրառմամբ գործող համակարգերի հետազոտության ժամանակ ծագող ինչպես ընդհանուր, այնպես էլ մասնավոր կարգի խնդիրներ, ձևակերպվել են այն խնդիրները, որոնց համապարփակ լուծմամբ կապահովվի ցանցային ենթակառուցվածքների վրա «հարձակումների մակերեսի» նվազարկումը:

Որպես ուսումնասիրության առանձին օբյեկտ հետազոտվել են ներխուժումների հայտնաբերման համակարգերում մեքենայական ուսուցման կիրառման արդյունավետությունը (արտադրողականությունը) չափելու հետազոտական խնդիրները ինչպես շարժական, այնպես էլ ներկառուցված համակարգերի համար: Ներկայացվել են ՆՀՀ-ներում մեքենայական ուսուցման կիրառման ուսումնասիրության աշխատանքում կատարված բարելավումները:

Այս խնդիրների լուծումը կբարձրացնի ցանցային ենթակառուցվածքի կայունության աստիճանը հնարավոր կամ հավանական ցանցակենտրոն հակամարտության դեպքում:

АНАЛИЗ НЕКОТОРЫХ ЗАДАЧ ПРИМЕНЕНИЯ МАШИННОГО ОБУЧЕНИЯ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КИБЕРСФЕРЕ

Т. В. ДЖАМГАРЯН, подполковник, старший офицер Управления связи и АСУ ВС РА

РЕЗЮМЕ

Одним из показателей четвертой промышленной революции является «цифровой блок», представляющий собой мост между физической и цифровой реальностями. Вся цифровая реальность представляет собой ряд устройств, объединенных сетями передачи данных. В связи с этим были исследованы угрозы сетевой инфраструктуре, в частности, с учетом некоторых особенностей сетецентрических войн.

Для нейтрализации разнородных угроз сетевой инфраструктуре используются программно-аппаратные решения, основанные на разных принципах и алгоритмах работы.

Были определены как общие, так и частные типы задач, возникающих при исследовании систем обнаружения вторжений (СОВ), действующих с использованием машинного обучения, а также сформулированы те задачи, всеобъемлющее решение которых обеспечит минимизацию «поверхности атак» на сетевые инфраструктуры.

В качестве отдельного объекта изучения были рассмотрены исследовательские задачи измерения эффективности (продуктивности) применения машинного обучения в системах обнаружения вторжений как для передвижных, так и для встроенных систем. Представлены поправки, внесенные в исследовательскую работу по применению машинного обучения в СОВ.

Решение подобных задач повысит степень устойчивости сетевой инфраструктуры в случае возможного или вероятного сетецентрического конфликта.

ANALYSIS OF SOME TASKS OF MACHINE LEARNING APPLICATIONS IN THE INTRUSION DETECTION SYSTEMS IN THE CYBER DOMAIN

T. V. JAMGHARYAN, Lieutenant Colonel, Senior Officer, Signal and AMS Department, the RA Armed Forces

SUMMARY

One of the indicators of the fourth industrial revolution is the “digital block”, which presents a bridge between the physical and digital realities. The entire digital reality is a series of devices connected with data networks. In this regard, threats to the network infrastructure were investigated, in particular, taking into account some peculiarities of network-centric wars.

Software and hardware solutions, based on different principles and operation algorithms, are used in order to neutralize various threats to the network infrastructure.

Tasks of both general and particular type, arising in the study of intrusion detection systems (IDS) and operating via machine learning were identified. In addition, the article formulated those tasks, the comprehensive solution of which will ensure the minimization of the “attack surface” on network infrastructures.

As a discrete object of study, the article discusses research problems of measuring the effectiveness (efficiency) of applying machine learning in intrusion detection systems for both mobile and embedded systems. The article dwells on the enhancements made to the research work on the application of machine learning in IDS.

The solution of such problems will increase the degree of stability of the network infrastructure in case a possible or probable network-centric conflict occurs.