«ՀԱԿԱԴՐԱՀԱՅԱՑ ՎԵՐԼՈՒԾՈՒԹՅՈՒՆԸ»՝ ՈՐՊԵՍ ՊԱՇՏՊԱՆԱԿԱՆ-ԱՆՎՏԱՆԳԱՅԻՆ ՀԱՄԱԿԱՐԳԵՐԻ ԳՆԱՀԱՏՄԱՆ ՄԵԹՈԴ

Կ. Ա. ԳԱԼՈՅԱՆ, քաղաքական գիտությունների թեկնածու, ՀՀ ՊՆ ԱՌՀԻ-ի կիբեռանվտանգության խմբի գիտնական-վերլուծաբան

Անվտանգության դեմ ուղղված սպառնալիքների որոշման, գնահատման, չեզոքացման և պետության կայուն զարգացման ապահովման համար անհրաժեշտ հիմնական ձեռնարկումներն արտացոլված են լինում ազգային անվտանգության ռազմավարություններում: Դրա մշակման ժամանակ կիրառվող էական գործիքներից է այլընտրանքային վերլուծությունը[*]: Այն ներառում է ինչպես ավանդական, այնպես էլ նորամուծական մեթոդներ, ինչպիսիք են սցենարային պլանավորումը, ՍՎՈՏ-ը, ԴԵԼՖԻ-ն, «հակադրահայաց վերլուծությունը»: Նշված մեթոդներից համեմատաբար քիչ է ուսումնասիրված «հակադրահայաց վերլուծությունը» («կարմիր թիմի» մեթոդիկա՝ *red teaming)*, որը հակառակորդի (մրցակիցների) դիտանկյունից յուրային հնարավորությունները, կարողությունները, ծրագրերը, ռազմավարությունն ու քաղաքականությունը ուսումնասիրելու, հասկանալու և թույլ կողմերը բացահայտելու մեթոդ է[1]: Այսպես. չինացի զորավար, տեսաբան, ռազմագետ և մտավորական Սուն Ցզին (մ. թ. ա. 544–496 թթ.) «Պատերազմի արվեստը» հայտնի աշխատության մեջ գրում է. «Ճանաչիր թշնամուդ և ինքդ քեզ ու հարյուրավոր պատերազմներում երբեք չես պարտվի… երբ անիրազեկ ես թշնամուդ մասին, բայց ճանաչում ես ինքդ քեզ՝ պարտվելու կամ հաղթելու հավանականությունը հավասարվում է: Եթե չես ճանաչում ո՛չ թշնամուն, ո՛չ էլ ինքդ քեզ՝ կպարտվես բոլոր ճակատամարտերում»[2]:

«Հակադրահայաց վերլուծությունն» առաջին անգամ կիրառվել է 19-րդ դարի

[*] Այլընտրանքային վերլուծությունը նպատակին հասնելու համար բազմազան տարբերակների վերհանումն ու գնահատումն է, դրանց արդյունավետության որոշումը (տես «Rethinking «Alternative Analysis» to Address Transnational Threats». The Sherman Kent Center for Intelligence Analysis Occasional Papers: October 2004, Vol. 3, N 2 (https://www.cia.gov/library/kent-center-occasional-papers/vol3no2.htm#_ftnref2)):

[1] Տես «Red Teaming and Alternative Analysis». «Red Team Journal» (http://redteamjournal.com/about/red-teaming-and-alternative-analysis/); «The Information Design Assurance Red Team (IDARTTM)». «Sandia National Laboratories», 2009 (http://www.idart.sandia.gov/): «Red team» («կարմիր թիմ»). արևմտյան մասնագիտական գրականության մեջ և զորավարժություններին վերաբերող այլ փաստաթղթերում խորհրդանշում է հակառակորդին:

[2] Տես *Sun Tzu*. The art of War. Translated and with an introduction by Samuel B. Griffith. Oxford University Press. New York and Oxford, P. 84 (http://web.stanford.edu/class/polisci211z/1.1/Sun%20Tzu.pdf):

առաջին տասնամյակներին պրուսական Գլխավոր շտաբում այն բանից հետո, երբ 1806 թ. հոկտեմբերի 14-ին՝ մեկ օրվա ընթացքում, Նապոլեոնի բանակը ծանր պարտության մատնեց պրուսական բանակին Ենայի և Աուերշտադտի ճակատամարտերում: Այդ ջախջախիչ պարտության դասերի հաշվառմամբ պրուսական ռազմական ոլորտում ձեռնարկվեցին բարեփոխումներ, որոնք 1820 թ. հանգեցրեցին առաջին ռազմական խաղի *(Kriegspiel)* ստեղծմանը՝ ինչպես տեղանքի, այնպես էլ հեծելազորի, հրետանու և հետևակի գործողությունների նմանարկմամբ: 1820-ական թվականներին խաղը ներկայացվեց Գլխավոր շտաբի պետ գեներալ ֆոն Մյուֆլինգին, որը նշեց. «սա խաղ չէ, այլ պատերազմին նախապատրաստում. այն մեծ արժեք ունի ամբողջ բանակի համար»[3]:

Կախված խնդրի բարդությունից՝ «կարմիր թիմը» կարող է բաղկացած լինել 2–25 անդամներից, մինչդեռ օպտիմալ թիվը 5-9 է: «Կարմիր թիմի» անդամները պետք է օժտված լինեն զարգացած դատողականությամբ և երևակայությամբ, ռազմավարական, քննադատական և ստեղծագործական մտածողությամբ, վերլուծական հմտություններով, այդ թվում՝ երևույթները տարբեր տեսանկյուններից դիտելու և գնահատելու հմտությամբ, ավանդական (կարծրատիպային) մտածելակերպին մարտահրավեր նետելու ունակությամբ, հաղորդակցային և ինքնակառավարման հմտություններով: Այսպիսով՝ կան մի շարք հանգամանքներ, որոնք կարող են ազդել «կարմիր թիմի» գործունեության որակի վրա:

«Հակադրահայաց վերլուծությունը» կատարվում է հետևյալ քայլերով.

1. նշանակվում է «կարմիր թիմի» ղեկավար, որը գերազանց կերպով տիրապետում է «կարմիր թիմի» մեթոդի կիրառման տեխնիկային,
2. կազմվում է «կարմիր թիմը»,
3. «կարմիր թիմը» ապահովվում է անհրաժեշտ տեղեկույթով,
4. «կարմիր թիմին» ներկայացվում են կոնկրետ նպատակները, ուսումնասիրության շրջանը, ժամանակացույցը և առաջադրանքի կատարման մեխանիզմները,
5. վերլուծության արդյունքները ներկայացվում են որոշում կայացնողներին,
6. ապահովվում է «կարմիր թիմի» աշխատանքների կառուցողական տացքը[4]:

«Կարմիր թիմը» կիրառական վերլուծությունը կատարում է երեք հիմնական փուլերով.

1. **ախտորոշման փուլ,** երբ ճշգրտվում են տեղեկույթի հավաստիությունը, մշակվում են պայմանական տրամաբանական նախադրույթները,
2. **ստեղծագործական փուլ,** երբ դիտարկվում են բոլոր հնարավոր սցենարները և դրանց հետևանքները,
3. **մարտահրավերի փուլ,** երբ դիտարկվում է վերլուծվող սցենարների համար առաջարկվող լուծումների հավաստիությունը[5]:

[3] Տես *Williamson Murray*. War, Strategy, and Military Effectiveness. Cambridge University Press. New York, 2011, P. 144:

[4] Տես «Red teaming guide». Ed. 2. Ministry of Defense, U.K. Development, Concepts and Doctrine Centre, January 2013, PP. 2-1, 2-2 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/142533/20130301_red_teaming_ed2.pdf):

[5] Տես նույն տեղում, էջ 3-2:

Յուրաքանչյուր փուլից հետո «կարմիր թիմը» պետք է վերանայի վերլուծության ընթացքը, որպեսզի պարզի, թե արդյոք ի հայտ չի եկել նոր տեղեկույթ:

Տվյալ մեթոդը կիրառելի է ինչպես պաշտպանական-անվտանգային, այնպես էլ պետության կայուն զարգացումն ու կենսագործունեությունն ապահովող մյուս բոլոր ոլորտների համար և կարող է նպաստել քաղաքական առաջնորդների, մասնավոր ընկերությունների ղեկավարների գործունեության արդյունավետության մակարդակի բարձրացմանը: Ներառելով այնպիսի գործիքներ, ինչպիսիք են մոդելավորումը, նմանարկումը, խոցելիության խորազննումը *(vulnerability probes)*՝ վերլուծության տվյալ մեթոդը հնարավորություն է տալիս մրցակցային միջավայրում բացահայտելու իր թույլ կողմերը, հավանական մարտահրավերներն ու սպառնալիքները և գտնելու դրանք չեզոքացնելու կամ ազդեցությունը հնարավորինս նվազեցնելու մեխանիզմներ:

Ներկայումս պաշտպանական-անվտանգային ոլորտում կատարվող վերլուծությունների ժամանակ «հակադրահայաց վերլուծությունը» կարող է կիրառվել ռազմավարական, մարտավարական և օպերատիվ մակարդակներում[6]: Դրա արդյունավետությունն ապահովելու համար կարևոր են ճիշտ հարցադրումները, որոնք խթանում են նորարարական մտածողության զարգացումը: Միևնույն ժամանակ, անհրաժեշտ է հարցադրումները ձևակերպել այն պայմանների համար, որոնցում կատարվում են նաև հիմնական սցենարային դիտարկումները՝ ոչ միայն ռազմական, այլև աշխարհագրական, քաղաքական, տնտեսական, սոցիալական և այլ առանձնահատկությունների հաշվառմամբ: Մեթոդի արդյունավետ կիրառման պարագայում հնարավոր է դառնում էապես կատարելագործել որոշումների կայացման գործընթացը: Մասնավորապես՝ մեթոդը կիրառելի է հայեցակարգերի մշակման, օպերատիվ պլանավորման, հետախուզության, ռեսուրսների կառավարման, տեխնիկական կարողությունների գնահատման գործում:

«Հակադրահայաց վերլուծությունը» հաջողությամբ կիրառվել է Գերմանիայում: 1919 թվականին կնքված Վերսալի պայմանագրով Գերմանիան զրկվել էր զրահապատ տրանսպորտային միջոցներ գնելու կամ նախագծելու հնարավորությունից: Սակայն գերմանացիները ներբերեցին զրահապատ մեքենաների արտադրման ոլորտում առաջատար բրիտանացիների փորձը: Քննադատորեն դիտարկելով առաջին աշխարհամարտի դասերը՝ գերմանացիներն սկսեցին հետազոտություններ, որոնց ընթացքում կիրառվեց «հակադրահայաց վերլուծությունը»: Նշված հետազոտությունները առանցքային նշանակություն ունեցան նաև գերմանական «կայծակնային պատերազմի» *(blitzkrieg)* ժամանակ ռազմական գործողությունների հավանական սցենարների մշակման համար[7]:

«Հակադրահայաց վերլուծությունը» հաջողությամբ կիրառվել է նաև 1962 թ. Կուբայի ճգնաժամի ժամանակ: Ճգնաժամի ծագման հենց առաջին օրը՝ հոկտեմ-

[6] Տես «Defense Science Board Task Force on The Role and Status of DoD Red Teaming Activities». DoD, Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics. Washington, September 2003, P. 2 (http://fas.org/irp/agency/dod/dsb/redteam.pdf):

[7] Տես «Defense Science Board Task Force on The Role and Status of DoD Red Teaming Activities», P. 31 (http://fas.org/irp/agency/dod/dsb/redteam.pdf):

բերի 16-ին, Նախագահ Քենեդին ձևավորեց Ազգային անվտանգության խորհրդի գործադիր կոմիտե, որի հիմնական նպատակն էր ստեղծված իրավիճակում այլընտրանքային մարտավարական սցենարների մշակումը՝ ի հակադրություն հակահարվածի առկա ռազմական սցենարի[8]:

Պաշտպանական-անվտանգային ոլորտում տեղեկատվահաղորդակցային տեխնոլոգիաների (ՏՀՏ) ներդրումը և կիրառումը անհրաժեշտություն են առաջ բերում «հակադրահայաց վերլուծությունը» կիրառելու նաև տվյալ ոլորտում առկա բացերի, հնարավոր սպառնալիքների բացահայտման համար: Այս մեթոդի տարատեսակն է «կիբեռ հակադրահայաց վերլուծությունը», որը կիբեռաշխարհում *(cyber world)* հարձակվողների մտածելակերպի և գործողությունների նմանարկմամբ հնարավորություն է տալիս պարզելու յուրային կիբեռանվտանգային հնարավորությունները և կատարելագործելու առկա կիբեռպաշտպանության մեխանիզմները: Միևնույն ժամանակ, հարկ ենք համարում նշել, որ կիբեռաշխարհում «հակադրահայաց վերլուծության» կիրառումը նոր երևույթ չէ: ԱՄՆ-ի Ազգային անվտանգության գործակալությունը տվյալ մեթոդը կիրառել է դեռ 1997 թ.: Դրա շնորհիվ հաջողվել է պետության համար կարևոր նշանակություն ունեցող ենթակառուցվածքներում (մասնավորապես՝ էներգետիկ ոլորտում) որոշարկել և գնահատել առկա սպառնալիքները: Այն, որ ԱՄՆ-ի Ազգային անվտանգության գործակալությունը կիրառեց «կիբեռ հակադրահայաց վերլուծությունը», ԱՄՆ-ի բարձրաստիճան պաշտոնյաների համար դարձավ նախադեպ: Ներկայումս ԱՄՆ-ի Պաշտպանության դեպարտամենտում «կիբեռ հակադրահայաց վերլուծության» կիրառումը կրում է պարբերական բնույթ: Դրա հիմնական նպատակը «կապույտ թիմերի» (յուրային) այն հնարավորություններն են, որոնք պետք է իրացվեն ցանցերը պաշտպանելու համար: Դա արվում է չորս հիմնական փուլերով (տես գծապատկերը):

«Կիբեռ հակադրահայաց վերլուծությունը» 2010 թվականից կիրառվում է Էստոնիայում տեղաբաշխված ՆԱՏՕ-ի գերազանցության կենտրոնի կազմակերպած «Կողպված վահաններ» *(Locked shields)* վարժանքների ժամանակ, որոնց նպատակն է տեղեկատվական համակարգերի խոցելի տեղերի բացահայտումը[9]:

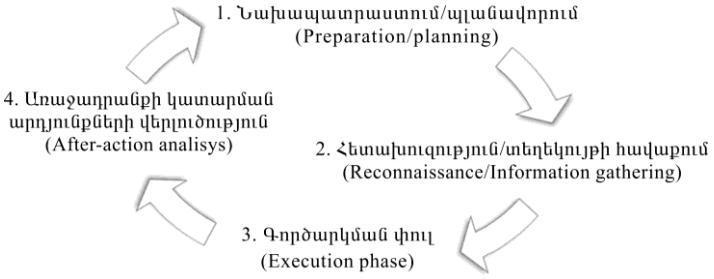
«Կարմիր թիմի» գործունեությունը բացառապես կապված է մարդկային ռեսուրսների հետ, և հաճախ բավական դժվար է լինում հավաքել իրազեկ «կարմիր թիմ», քանի որ հայրենական մասնագետները սովորաբար լինում են սակավաթիվ, մինչդեռ որոշումների կայացման տարբեր մակարդակներում անհրաժեշտ են կոնկրետ բարձրակարգ մասնագետներ[10]: ՈՒստի անվտանգային հետազոտություններում կիրառվում է նաև «կարմիր գործակալի» մոդելը, որը, լինելով համակարգչային ծրագիր, կարող է փոխարինել մարդուն կամ աջակցել մարդկանցով համալրված «կարմիր թիմի» գործունեությանը: Այս ավտոմատացված մոդելը մշակվում է հակառակորդի վարքագիծը կանխատեսելու և ռազմավարական

[8] Տես նույն տեղում, էջ 32:

[9] Տես նույն տեղում, էջ 14:

[10] Տես *Paul K. Davis, William L. Schwabe.* Search for a Red Agent to be Used in War Games and Simulations. «RAND» corporation, July 1985, P. 1:

խաղերի ու նմանարկումների ժամանակ կիրառելու համար: Խաղային կառուցվածք ունեցող նմանարկումները կարող են բաղկացած լինել բազմաթիվ բարդ և տարաբնույթ սցենարներից, որոնց մշակման գործը դյուրինացվում է ռազմավարական խաղի ավտոմատացման շնորհիվ:



Գծապատկեր. «Կիբեռ հակադրահայաց վերլուծության» փուլերը[11]

Այսպիսով՝ այլընտրանքային վերլուծության՝ «կարմիրների թիմի» և «կարմիր գործակալի» մեթոդների կիրառումը կարող է արդյունավետ միջոց լինել պաշտպանական-անվտանգային ոլորտի պրոբլեմների վերհանման և սպառնալիքների դեմ արդյունավետ պայքարի կազմակերպման ու գնահատման համար:

[11] Տես *Pascal Brangetto, Emin Çalişkan, Henry Rõigas.* Cyber Red Teaming: organizational, technical and legal implications in a military context. NATO Cooperative Cyber Defense Centre of Excellence. Tallinn, 2015, P. 7:

ПОЛИТОЛОГИЧЕСКИЕ ИССЛЕДОВАНИЯ

«АНАЛИЗ С ПОЗИЦИЙ ПРОТИВНИКА» КАК МЕТОД ОЦЕНКИ ОБОРОННО-БЕЗОПАСНОСТНЫХ СИСТЕМ

К. А. ГАЛОЯН, кандидат политических наук, ученый-аналитик Группы кибербезопасности ИНСИ МО РА

РЕЗЮМЕ

Одним из эффективных альтернативных методов анализа состояния системы безопасности организации (государства, предприятия, иного субъекта конкурентных отношений) является метод «анализа с позиций противника» (методика «красных команд»). Его сущность заключается в оценке существующих угроз, возможностей их парирования, разрабатываемых и уже реализуемых стратегий и политики глазами противника (конкурента) в целях определения их сильных и слабых сторон, в первую очередь – уязвимых точек.

В последние годы этот метод получает все большее применение при решении безопасностных вопросов, однако он используется и для экспертного обеспечения устойчивого развития во всех сферах жизнедеятельности

государства и общества. «Анализ с позиций противника» позволяет выявить основные недостатки, вызовы, возможности и потенциальные угрозы в условиях конкурентной среды, детерминировать возможные оборонные сценарии на стратегическом, тактическом и оперативном уровнях, найти оптимальные решения посредством применения механизмов моделирования и имитирования, а также проверки на уязвимость.

Данный метод получил широкое распространение и в сфере кибербезопасности, где, в частности, модель «красного агента» представляет собой компьютерную программу для оценки кибер возможностей, разработок информационных технологий и перспектив защиты информационной инфраструктуры посредством разработки сценариев и моделирования кибератак в целях обнаружения уязвимых мест в сети и системе.

POLITICAL STUDIES

"RED TEAMING" AS A METHOD FOR ASSESSING DEFENSE-SECURITY SYSTEMS

K. A. GALOYAN, PhD in Political Science, Research Fellow at the Cybersecurity Group, INSS, MOD, RA

SUMMARY

One of the efficient alternative methods for the state analysis of security system of an organization (state, enterprise, or other entity of competitive relations) is the method of «the analysis from the position of an enemy» («red team» method). Its essence is in the assessment of the existing threats, the opportunities of countering them, the strategies and policy being developed and having been already implemented from an adversary's (competitor's) perspective for identifying their strengths and weaknesses, firstly – vulnerabilities.

In recent years this method has been increasingly used in security affiliated issues, however it is also applicable for the expert provision of sustainable development in all fields of state and society activities. «The analysis from the position of an enemy» makes it possible to identify key weaknesses, challenges, opportunities and potential threats in a competitive setting, to reveal possible defense scenarios on strategic, tactical and operational levels, to find optimal solutions through the use of modeling and simulation mechanisms, as well as vulnerability probes.

This method also became widespread in the sphere of cybersecurity, where, particulary, a "red agent" model is a computer program for the evaluation of cyber capabilities, information technology developments and information infrastructure protection prospects through the development of scenarios and modeling of cyber attacks for detecting network and system vulnerabilities.