Գ Լ Ո Բ Ո Ւ Մ

ՎԵՐԼՈՒԾԱԿԱՆ ՏԵՂԵԿԱԳԻՐ

ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԽՆԴԻՐՆԵՐԻ ՇՒՐՋ

4

Մարտ

2008

«ՆՈՐԱՎԱՆՔ» ՀԻՄՆԱԴՐԱՄ

Գ Լ Ո Բ Ո Ւ Ս
Վերլուծական տեղեկագիր

Г Л О Б У С
Аналитический бюллетень

№ 4 (32)
Մարտ, 2008թ.

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

ՀՀ ՏԵՂԵԿԱՏՎԱԿԱՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅԱՆ ԽՆԴԻՐՆԵՐԻ ՇՈՒՐՋ

Ներկայիս գլոբալացման գործընթացների առաջնային հատկանիշներից է համաշխարհային տեղեկատվական-հաղորդակցական ընդհանուր դաշտի ձևավորումը: Որպես հետևանք՝ ազգային-պետական տեղեկատվական դաշտի[1] սահմանների այսպես կոչված «տեխնիկական պաշտպանությունը», չնայած որոշ երկրներում կատարվող փորձերի[2], կապված է լուրջ բարդությունների հետ: Այստեղից հետևում է, որ պետության և հանրության լիարժեք տեղեկատվական անվտանգությունը (ՏԱ) կարող է պայմանավորված լինել բացառապես սեփական տեղեկատվական ռեսուրսների (մտավոր, հոգևոր և տեխնիկական) հնարավորություններով և այդ ռեսուրսների միջոցով ձևավորված տեղեկատվական դաշտի համակարգված ներուժով:

Միասնական տեղեկատվական դաշտի խնդիրները

Հայաստանի (ՀՀ, ԼՂՀ և, թերևս, նաև Ջավախքի) ՏԱ ոլորտի առաջնային խնդիրներից է միասնական տեղեկատվական դաշտի ձևավորումը: Հայտնի է, որ ներկայիս ներքին լրատվական հոսքերը հիմնականում վերաբերում են մայրաքաղաք Երևանին և գրեթե չեն լուսաբանում իրավիճակն Արցախում, Ջավախքում և ՀՀ մարզերում: Թերևս, ժամանակն է վերականգնելու այսպես կոչված սեփական թղթակիցների ինստիտուտը, որը ժամանակին հնարավորություն էր տալիս Հայաստանի բնակչությանն իրազեկ լինել այս կամ այն շրջանում կատարվող իրադարձություններին: Այս ոլորտում պետք է կարևորել նաև միասնական տեղեկատվական դաշտի բովանդակության խնդիրը. գաղտնիք չէ, որ թերացումներն այստեղ բազմաթիվ են, ինչը վտանգում է հանրության և անձի իրազեկ լինելու իրավունքը: Իրազեկության խնդրի համատեքստում պետք է դիտարկել նաև բաց աղբյուրներից ստացվող տեղեկատվության հոսքերի նպատակային մշակումը և այն պետական մարմիններին տրամադրելու հիերարխիկ համակարգի ձևավորումը[3]:

Միասնական տեղեկատվական դաշտի ձևավորումը նույնքան հրատապ է նաև Համաշխարհային Հայության անվտանգության համատեքստում: Սակայն այս խնդրի լուծումը, հասկանալի պատճառներով (բավական է նշել, որ Հայությունը սփռված է ավելի քան հարյուր երկրներում, և մի քանի հարյուրի հասնող համայնքների թիվն անգամ ճշգրիտ հայտնի չէ), անհամեմատ ավելի բարդ է: Այս ուղղությամբ աշխատանքները, իհարկե, ենթադրում են սփյուռք ունեցող այլ ժողովուրդների, մասնավորապես՝ հրեաների փորձի ուսումնասիրություն: Կարծում ենք նաև, որ Հայության միասնական տեղեկատվական դաշտի ձևավորման խնդիրը կարող է իրատեսական լինել միայն ՀՀ ՏԱ հայեցակարգի և համակարգի ստեղծումից հետո միայն:

---

[1] Այս բառակապակցությամբ հետագա շարադրանքում նկատի կունենանք ՋԼՄ-ի, Ինտերնետի և տեղեկատվության այլ աղբյուրների միջոցով ձևավորված դաշտը:

[2] Ուսանելի է, մասնավորապես, Չինաստանի փորձը, որտեղ արգելանքներ են դրվել հանրության բարոյականության նորմերը խախտող տեղեկատվական հոսքերի դեմ:

[3] Նկատենք, որ նման համակարգ (մասնավորապես, ԱՏԼԱՍ անվանումը կրող) գործում էր ԽՍՀՄ-ում, որի միջոցով պետական և կուսակցական ընտրանին (այսպես կոչված նոմենկլատուրան) բավական օբյեկտիվ տեղեկատվություն էր ստանում միջազգային քաղաքական զարգացումների վերաբերյալ: Անշուշտ, տեղեկատվական դաշտում վերջին տասնամյակում էական փոփոխություններ են տեղի ունեցել, սակայն խորհրդային փորձը, ըստ մեզ, ուսանելի է առայսօր:

Ինֆոգեն սպառնալիքների հետ կապված խնդիրներ

Ընդունված է համարել, որ Հայաստանի և Հայության անվտանգությանը սպառնացող արտաքին ինֆոգեն (տեղեկատվածին) սպառնալիքների աղբյուրները գլխավորապես մի քանի ադրբեջանական և թուրքական լրատվամիջոցներ են: Նման մոտեցումը, անշուշտ, պարզունակ է: Սակայն անգամ վերոնշյալ լրատվամիջոցների կողմից սփռվող ակնհայտորեն սադրիչ տեղեկատվական հոսքերը չեն ենթարկվում փորձագիտական վերլուծության, չեն բացահայտվում դրանց տեխնոլոգիական և մեթոդաբանական առանձնահատկություններն ու ընդհանրությունները: Մինչդեռ, առանց նման աշխատանքի անհնարին է բացահայտել ինֆոգեն սպառնալիքների իրական կենտրոնները, հասկանալ նրանց նպատակները և ռազմավարությունը: Ակնհայտ է, որ այդ ոլորտում պետք է օգտագործել անհրաժեշտ գիտելիքների ձեռքբերման ընդունված մեխանիզմները (ուսուցում արտասահմանյան կենտրոններում, փորձագետների հրավիրում և այլն) ու կիրառել դրանք գործնական հարթությունում:

Այս ամենի առիթով պետք է շեշտել, որ ուշադրության արժանի տեղեկատվության ոլորտները և խնդիրները տարաբնույթ են, ու դրանք ժամանակի հետ բազմանում են արագացումով: Բավական է նշել վերջին տասնամյակում մոբիլ հեռախոսների լայն տարածման շնորհիվ գոյացած այսպես կոչված «երրորդ էկրանի» (հեռուստացույցի և համակարգչի էկրաններից հետո) խնդիրը. *SMS* հաղորդագրությունները 2006թ. արաբա-իսրայելական հակամարտության ընթացքում երկուստեք լայնորեն օգտագործվում էին որպես կարևոր տեղեկատվական-հոգեբանական ներգործության միջոց: Մինչդեռ մեր փորձագիտական հանրությունում գրեթե չեն շոշափվում հանրապետության տեխնիկական-էլեկտրոնային համակարգերի դեմ ուղղված ինֆոգեն սպառնալիքների հակազդեցության խնդիրները[4]:

Հստակեցման կարիք ունեն նաև ներքին տեղեկատվական դաշտում[5] գործող իրավաբանական նորմերը. տեղեկատվական գործողությունները երբեմն ներկայացվում են որպես զուտ ժողովրդավարության և խոսքի ազատության իրավունքի արտահայտում: Մինչդեռ քիչ չեն դեպքերը, երբ դրանք իրենց բովանդակությամբ և ձևով կրում են մանիպուլյատիվ բնույթ և ուղղված են մեր ազգային շահերի դեմ: Հարկ է նկատել, որ նման տեղեկատվական-հոգեբանական գործողությունները մի շարք արևմտյան՝ այսպես կոչված «զարգացած ժողովրդավարության» երկրներում ենթակա են քրեական հետապնդման: Այս առիթով նշենք, որ այս նախագահական ընտրություններում թեկնածուներից մեկը հնչեցրեց ԼՀՂ խնդրի կարգավորման, ինչպես նաև Ադրբեջանի և Թուրքիայի հետ հարաբերությունների վերաբերյալ քաղաքական թեզեր ու մոտեցումներ, որոնք ժամանակավոր զինադադարի կարգավիճակում գտնվող մեր երկրի պարագայում պետք է ստանային նաև իրավական գնահատական:

Տեսական խնդիրներ

ՏԱ տեսական ոլորտը, անշուշտ, խիստ կարևոր է: Բավական է նշել, որ այսօր բացակայում են տեղեկատվական գործողությունների կամ պատերազմների վերաբերյալ միանշանակ և բոլորի կողմից ընդունված սահմանումներ: Որպես հետևանք՝ այդ հասկացությունները մեր հանրությունում և, մասնավորապես, վարչական մարմինների տարբեր օղակներում, հաճախ ընկալվում են ոչ ադեկվատ ու մեկնաբանվում են յուրովի: ՏԱ համակարգի ձևավորման

---

[4] Այս կապակցությամբ տեղին է նշել, որ համաձայն ԶԼՄ-ի, ս.թ. հունվարին ԱՄՆ նախագահը ստորագրել է ՏԱ տեխնիկական ոլորտին վերաբերող երկու դիրեկտիվ, համաձայն որոնց, մասնավորապես, ամերիկյան հատուկ ծառայություններն իրավունք են ձեռք բերում նախահարձակ տեղեկատվական գործողություններ ձեռնարկել ԱՄՆ անվտանգությանը սպառնացող կենտրոնների դեմ:

[5] Նկատենք, որ գլոբալ տեղեկատվական հարթությունում միջազգային իրավունքի համապատասխան նորմերը մշակված չեն: Մինչդեռ խնդիրը հրատապ է և շարունակաբար քննարկվում է միջազգային տարբեր ատյաններում: Այս հարցում Հայաստանը, որպես տեղեկատվական պատերազմների սուբյեկտ, պետք է փորձի ակտիվ մասնակցություն ունենալ: Միևնույն ժամանակ, գործնական հարթությունում հիմնական շեշտը պետք է դրվի տեղեկատվական ոլորտին վերաբերող ներքին իրավաբանական դաշտի ձևավորման հարցերի վրա:

առաջին փուլերում, թերևս, անհրաժեշտ է օգտվել այդ ոլորտում համբավ վայելող հեղինակների (օրինակ՝ Թոմաս Ռոնիի, Սերգեյ Գրինյանի) կողմից ՏԱ հասկացություններին տրված մասնագիտական սահմանումներից։ Նման մոտեցումը, անշուշտ, ենթադրում է համապատասխան եզրաբանական բառարանի ստեղծում։

Այս ամենին զուգահեռ, պետք է մշտապես հիշել, որ փորձագիտական հանրությունում անվերապահորեն ընդունված է այն դրույթը, թե ՏԱ ոլորտում, առավել քան այլ բնագավառներում, պետք է խուսափել այլ երկրների փորձի կույր փոխառությունից, քանի որ տեղեկատվական խնդիրներն ուղղակիորեն խարսխված են անհատի և ազգի հոգեկերտվածքի վրա ու մեծապես կախված են երկրի աշխարհաքաղաքական իրավիճակից։

Որոշ հետևություններ

ՏԱ խնդիրներով մեր հանրությունում հիմնականում զբաղվում են միայն առանձին անհատներ։ Նրանցից ոմանք ունեն բարձր պրոֆեսիոնալ մակարդակ և սեփական աշխարհայացքային սկզբունքներից ելնելով ամենօրյա տեղեկատվական-քարոզչական աշխատանք են վարում ու հնարավորինս դիմակայում տեղեկատվական հարձակումներին։ Սակայն այդ առանձին անհատների գործունեությունը կրում է իրավիճակային, մարտավարական բնույթ։ Որպես հետևանք՝ քիչ չեն դեպքերը, երբ այս կամ այն քաղաքական խնդրի նկատմամբ ընդհանուր մոտեցումների բացակայությունը փոշիացնում է այդ անհատների ջանքերը։

Ըստ մեզ՝ տեղեկատվական քաղաքականության մշակումը ենթադրում է, առաջին փուլում, փորձագիտական մի հանձնաժողովի ստեղծում, որը կհաշվառի ինչպես մեր ունեցած տեղեկատվական ռեսուրսները, այնպես էլ ՏԱ ոլորտի հիմնախնդիրները։ Հանձնաժողովի աշխատանքից ստացված արդյունքները կարող են հիմք հանդիսանալ քաղաքական ղեկավարության համար՝ քայլեր կատարելու ՏԱ համակարգի ենթակառուցվածքի ձևավորման ուղղությամբ։ Դա ենթադրում է, մասնավորապես, պետական հովանավորություն ունեցող կառույցների ստեղծում։ Այս համատեքստում նշենք, որ ՀՀ Ազգային անվտանգության ռազմավարության և ՀՀ Ռազմական դոկտրինի փաստաթղթերի ստեղծումը գերազանցապես պայմանավորված էր Պաշտպանության նախարարության և նրա վերլուծական կառույցների առկայության փաստով։ Այսինքն՝ առանց մասնագիտացված կառույցների դժվար է պատկերացնել առաջխաղացում ՏԱ ոլորտի անգամ տեսական խնդիրների ուղղությամբ։

Գագիկ Հարությունյան
«Նորավանք» հիմնադրամ

ՀՀ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԹԵՄԱՅԻ ՇՈՒՐՋ

Տեղեկատվական անվտանգության հիմնախնդիրն ունի առաջնային կարևորություն և պետական իշխանության ուշադրության կենտրոնում է: Դա առավել ընդգծված է դառնում այն պարագայում, երբ տվյալ երկիրը գտնվում է պատերազմական վիճակում, ինչպես ՀՀ-ն է: Մյուս կողմից՝ Հայաստանի համար այս թեման առավել ևս կարևոր է՝ հաշվի առնելով, որ մեր երկիրն առայժմ այս առումով որոշ իմաստով խոցելի է արտաքին տերությունների համար, քանի որ հակազդման մեխանիզմները կայացման փուլում են:

Ներկայացնենք որոշ նկատառումներ, որոնք, գուցե, կարող են օգտակար լինել տեղեկատվական անվտանգության և տեղեկատվական պատերազմների տեսանկյունից.

- Նպատակահարմար է թվում սկսել միջազգային մամուլի պարբերական մոնիթորինգ և վերլուծություն, ուսումնասիրել Հայաստանի, Սփյուռքի թեմաներով, ԼՂ հակամարտության, Մեծ եղեռնի, հայ իրականության հետ առնչվող այլ հոդվածներն ու լուրերը, արձանագրել դրանց սկզբնաղբյուրները, հեղինակներին: Այս մեթոդով մոտ 2-3 ամսվա ընթացքում հնարավոր է ստանալ որոշակի պատկեր հակահայ և հայանպաստ հրապարակումների և միջազգային ԶԼՄ-ի, ադրբեջանա-թուրքական կողմի հակահայ տեղեկատվական-քարոզչական աշխատանքի մասին: Այս առումով արդիական են ռուսական զանգվածային լրատվամիջոցները, որոնցում, ըստ առկա տեղեկությունների, Բաքվի պատվերով հաջողվել է 2006թ. մայիսի 27-ին՝ Ադրբեջանի 1-ին հանրապետության օրը, հրապարակումներ տպագրել: Հայտնի է նաև, որ Ադրբեջանին հաջողվել է նաև, վճարովի հիմունքներով, հունգարական «Դունա» հեռուստաալիքի եթերում 12-ժամյա տեսանյութեր հեռարձակել երկրի վերաբերյալ: Դա տեղի է ունեցել պետական նախաձեռնությամբ. «Դունա» հեռուստաալիքի ղեկավար անդամներից Լասլո Չելինին հրավիրվել էր Բաքու: 2007թ. սեպտեմբերի 21-ին նույն հեռուստաալիքը 12 ժամ անվճար հեռուստաեթեր է տրամադրել հայկական կողմին: Այն կազմակերպվել էր Հունգարիայի հայկական համայնքի ջանքերով՝ Հայաստանի Հանրային հեռուստատեսության որոշակի աջակցությամբ: Առանցքային նշանակություն է ունեցել Լասլո Չելինիի մոտեցումը. վերջինս համակրանք ունի հայ ժողովրդի հանդեպ, ըստ որոշ տվյալների՝ հնարավոր է, որ հայկական ծագում ունենա: 2007թ. օգոստոսին Միացյալ Նահանգների թերթերից մեկն անդրադարձավ ԱՍԱԼԱ-ի թեմային՝ թուրքամետ և ադրբեջանամետ շեշտադրումներով: Վստահաբար, այս հրապարակումը ևս պատվերի շրջանակում էր: Այս առումով հետաքրքրական է, թե միջազգային որ ԶԼՄ-ում տեղ կգտնեն անդրադարձներ Խոջալիի դեպքերի տարելիցի առիթով:
- Նպատակահարմար է թվում, որպեսզի առավել ընդլայնվի այն հայ փորձագետների, քաղաքագետների թիվը, որոնք կարող են, անհրաժեշտության պարագայում, հանդես գալ այնպիսի հրապարակային ելույթներով, որոնք հարկավոր են տեղեկատվական-քարոզչական աշխատանքի, ադրբեջանա-թուրքական կողմի հետ «տեղեկատվական պատերազմի» նկատառումներով: Այս մեթոդը լայնորեն կիրառվում է միջազգային պրակտիկայում, մասնավորապես՝ Թուրքիայում, իսկ վերջին շրջանում բավական զարգացել է Ադրբեջանում: Որոշ թվով փորձագետներ՝ ռազմական հարցերով փորձագետ Ուզեիր Ջաֆարով, Յաշար Ջաֆարլի, Սամեդ Վուրղունով, անհրաժեշտության պարագայում, «պետպատվերի» շրջանակում կատարում են հայտարարություններ, որոնք տպագրվում են ԶԼՄ-ում: Դրանք նաև թարգմանվում են օտար լեզուներով և այսպիսով դրվում շրջանառության մեջ: ՀՀ-ում գործնականում կան նման քաղաքագետներ, փորձագետներ, սակայն նրանց թիվը համեմատաբար սահմանափակ է: Հատկապես «ռազմական փորձագետների» առումով Ադրբեջանում առկա են մշտապես գործող

«խոսափողներ»՝ պաշտոնաթող փոխգնդապետ Ուզեիր Ջաֆարովը և Յաշար Ջաֆարլին, որոնք ելույթներ են ունենում հայկական բանակի, ՀՀ-ում առկա սպառազինությունների, ՀՀ-ի կողմից հրադադարի խախտման, հայ-ռուսական ռազմական փոխգործակցության թեմաներով, հանդես են գալիս պատերազմի վերսկսման վտանգի մասին սպառնալի հայտարարություններով: Հայկական կողմի համար ռազմական, ռազմաքաղաքական, անվտանգության, ադրբեջանական բանակի ուղղությամբ մասնագետների կարիք կա:

- Ադրբեջանական կողմը հաճախակիացրել է հայկական կայքէջերի դեմ ուղղված հարվածները: Վերջին տարիներին ադրբեջանական հաքերների հարվածներից տուժել են «Նորավանք» հիմնադրամի, «Հայաստան 2020» կազմակերպության, Հայաստանի Հանրային ռադիոյի, www.banks.am, www.armenia.com, www.yerevan.ru կայքերը: Ամենայն հավանականությամբ ցանկն ամբողջական չէ: Ըստ առկա տպավորության՝ հայկական կողմը դեռևս չի մշակել ռազմավարություն՝ հարձակումների դեպքում հասցնե՞լ համարժեք պատասխան հարված, թե՞ ոչ: Առկա է այլընտրանքային մոտեցում, որ պատասխանելը պարտադիր չէ, քանի որ հաքերային հարվածները վերջնահաշվում վերածվում են հայկական կայքէրի «զովազդի», և վերանորոգումից հետո տվյալ կայքի վարկանիշն աճում է: Սա, թերևս, կարևոր գործոն է: Մյուս կողմից՝ անպատասխան հարվածն ադրբեջանական կողմի համար հոգեբանական ազդակ է հանդիսանում, ուժի պատրանք և հայկական կողմի որոշակի թուլության տպավորություն ստեղծում: Դա, իր հերթին, ինչ-որ առումով օգնում է աստիճանաբար ազատվել «պարտվողի» կամ «զոհի» հոգեբանությունից, որն առկա էր Ադրբեջանում պատերազմին հաջորդած շրջանում: Թերևս, նպատակահարմար է քննարկել անհրաժեշտության դեպքում ադրբեջանական սայթերը շարքից հանելու ռազմավարության հարցը ևս:

2000թ. արբեջանական կողմի գործողություններից վնասվեցին մի շարք հայկական կայքեր, ինչին ի պատասխան հայկական կողմի «Լիազոր գրուփ» խումբը շարքից հանեց մի շարք ադրբեջանական թերթերի կայքէջեր: Դրան հաջորդած մոտ 2 տարվա ընթացքում Ադրբեջանը խուսափում էր նման «վիրտուալ պատերազմներից»: Մինչդեռ, անպատասխան թողնելու արդյունքում, վերջին շրջանում ադրբեջանական կողմն իրեն առավել ազատ և սանձարձակ է զգում: Նրա հաքերային հարվածները նաև ինչ-որ իմաստով ստվերում են ՀՀ-ի՝ տարածաշրջանում տեղեկատվական տեխնոլոգիաների կենտրոն դառնալու ռազմավարական ծրագիրը, թերևս նաև ազդում ՀՀ վարկանիշի վրա:

Պետք է նաև նկատի ունենալ, որ հայկական կողմի պատասխան հարվածներին առաջին շրջանում կարող են հաջորդել նոր հարվածներ Ադրբեջանի կողմից, և «վիրտուալ պատերազմը» կարող է երկարաձգվել: Այսպիսով, կարևոր է նաև ՀՀ կայքերի պաշտպանությունն ուժեղացնելու, ծրագրային մասն առավել ամրացնելու գործը:

Հայկարամ Նահապետյան

КОНТРРАЗВЕДЫВАТЕЛЬНЫЕ ОПЕРАЦИИ В КИБЕРПРОСТРАНСТВЕ[1]

В США планируется в 40 раз сократить количество правительственных интернет-порталов

В начале января Джордж Буш издал две секретные директивы за номерами 54 (Директива президента по национальной безопасности) и 23 (Директива президента по внутренней безопасности). В этих документах спецслужбам США и прежде всего Министерству внутренней безопасности (МВБ), а также Агентству национальной безопасности (АНБ) даются указания по усилению контроля над компьютерными сетями, используемыми американскими федеральными структурами. Кроме того, заокеанские разведчики и контрразведчики должны расширить сферы мониторинга информации, поступающей в сети правительственных ведомств Соединенных Штатов через интернет.

Предписано действовать согласованно

Разумеется, и прежде правительство США последовательно и поэтапно принимало меры по защите своих баз данных от хакеров всех мастей, организованных преступных группировок и иностранных разведок. Однако эти мероприятия реализовывались различными ведомствами, проводились ими самостоятельно и не были должным образом связаны друг с другом.

После подписания Бушем новых директив под руководством директора национальной разведки США была создана специальная структура, которой предписано осуществлять координацию усилий американских спецслужб по вскрытию источников кибернетических атак на федеральные информационные системы. МВБ будет обеспечивать защиту этих систем. А Пентагону надлежит разработать стратегию противодействия всем попыткам извлечения данных, потеря которых может повредить национальной безопасности страны.

За последние полтора года сети Государственного департамента, Министерства торговли, Минобороны и МВБ США неоднократно подвергались атакам хакеров и зарубежных спецслужб. Чиновники в Вашингтоне и специалисты по компьютерной безопасности утверждают, что крупнейшие атаки на все эти ведомства, включая базы данных некоторых лабораторий, занимающихся ядерными разработками, и крупных подрядчиков МО, были предприняты Китаем.

АНБ имеет богатый опыт наблюдения за большим количеством сложных зарубежных систем связи. Однако перспектива перенацеливания агентства на внутренние системы связи США вызывала серьезные возражения со стороны многих американских политиков. Серьезные дебаты велись и по вопросу контроля каналов передачи информации на территории США без получения соответствующих разрешений от судебных органов.

В рамках новых директив Буша МВБ будет осуществлять мониторинг всех попыток вскрытия информационных систем федеральных органов и вести соответствующие базы данных, где будут зафиксированы все случаи взлома сетей и используемых для этого технологий. В то же время планируется сократить число правительственных интернет-порталов с 2000 до 50, чтобы можно было эффективно отслеживать все нападения.

Кстати, вопрос о возложении ответственности за пресечение кибератак на МВБ дебатировался довольно долго. Еще в прошлом году Совет по обеспечению внутренней безопасности предложил администрации Белого дома передать этому министерству главные полномочия по защите американских компьютерных сетей. Однако данная инициатива была встречена в

[1] http://nvo.ng.ru/printed/205964. 08.02.2008.

штыки руководством различных ведомств разведывательного сообщества США. Они аргументировали свои возражения тем, что МВБ, созданное только в 2003г., не имеет необходимого опыта для решения подобных задач и не пользуется в спецслужбах США необходимым авторитетом. «Перетягивание каната» по этому вопросу продолжалось в течение нескольких недель, и в конце концов было принято окончательное решение в пользу МВБ.

Американские законодатели, занимающиеся разработкой регламентов по обеспечению внутренней безопасности и деятельности спецслужб США, заявили, что они в течение многих месяцев пытались добиться от администрации Буша подробных сведений по сути директив президента №54 и №23. Помощники парламентариев и бывшие сотрудники Белого дома, знакомые с содержанием программы Буша по противодействию атакам на национальные компьютерные сети, заявляют, что в упомянутых выше документах очерчен круг проведения мероприятий под общим названием «кибернетическая инициатива». На них предполагается истратить миллиарды долларов, которые будут запрошены в бюджете на 2009 финансовый год.

Разноречивые оценки

Представитель Белого дома Скотт Стензель заявил журналистам, что «директивы президента являются продолжением» усилий Вашингтона по обеспечению безопасности федеральных информационных систем и их защиты от постоянных попыток проникновения хакеров, террористов и иностранных спецслужб с целью извлечения конфиденциальных данных. Он также отметил, что предстоит большая работа по выявлению уязвимых мест государственных баз данных и выработке мер по организации эффективного противодействия ожидаемым угрозам. Однако чиновник не посвятил прессу в какие-либо детали новых требований Буша к разведке.

Один из представителей американских спецслужб объявил, что подразделения по защите информации АНБ, ЦРУ и ФБР будут заниматься расследованием всех попыток проникновения в федеральные базы данных путем постоянного отслеживания потоков информации, проходящей через интернет, а в отдельных случаях они должны копировать подозрительные сообщения для проведения дальнейшего анализа.

По словам того же источника, новыми директивами Буша Пентагону разрешается разрабатывать планы проведения кибернетических контратак на информационные сети противников США. В тех случаях, когда АНБ будет установлен конкретный факт нападения и выявлен сервер иностранного государства, с которого была осуществлена атака, специалисты Минобороны нанесут по нему ответный удар, чтобы прекратить новые атаки на информационные сети американского правительства. Такие же меры будут приниматься в тех случаях, когда атакам будут подвергаться сети частных фирм.

Бывший консультант по вопросам безопасности и советник президента США по обеспечению защиты критических элементов инфраструктуры Пол Кертц заметил, что Белый дом «сделал твердый шаг вперед на пути разработки мер кибероборонs». Он также подчеркнул, что все эти действия ни в коей мере не предполагают слежение за американскими гражданами. А председатель комитета внутренней безопасности Палаты представителей американского Конгресса Бенни Томпсон заявил, что «ведомства, основной задачей которых является сбор информации о зарубежных объектах, не должны заниматься мониторингом компьютерных систем» на территории Америки.

Алан Пэллер, владелец и директор американского Института компьютерной безопасности *SANS*, отметил, что если не включать в перечень охраняемых баз данных системы управления промышленностью, это будет означать, что у служб, занятых в данной сфере, «один глаз просто закрыт, поскольку хакеры используют одни и те же технологии для правительственных и коммерческих структур». «Если вы пытаетесь обнаружить иголку в стоге сена, вам необходимо перелопатить столько данных, сколько вы физически способны заполучить. Эти иголки действительно очень тонки, а плохие парни всеми мерами пытаются их надежно спрятать», – сказал Пэллер.

Сторонники принятия действенных мер по кибербезопасности утверждают, что изданные Бушем документы носят однобокий характер, поскольку в них нет указаний о постановке барьеров на пути проникновения в системы управления предприятиями частного сектора, очистительными предприятиями, банками и, что самое главное, объектами энергетического сектора страны. А возможные нападения на компьютерные сети в этих сферах составляют около 90% всех угроз национальной безопасности США.

При этом многие зарубежные эксперты отмечают, что попытки вторжения в сети правительственных органов вряд ли могут окончиться хаосом. Прежде всего потому, что все они имеют некие резервные системы управления, которые позволяют в большинстве случаев обеспечить непрерывность руководства страной. Кроме того, ни хакеры, ни террористы, ни зарубежные спецслужбы на сегодняшний день не обладают необходимыми техническим возможностями для нанесения глобального информационного удара по Америке. Однако ее энергетический сектор в этом смысле сегодня является одним из самых уязвимых мест.

В свою очередь, на конференции компаний, организованной Институтом компьютерной безопасности *SANS* в Новом Орлеане, представители компаний, занимающихся проблемами обеспечения компьютерной безопасности, в очередной раз предупредили о большой уязвимости таких важных элементов национальной инфраструктуры, как электросеть, транспорт, система водоснабжения, дамбы и некоторые другие жизненно важные объекты. Выступивший перед собравшимися экспертами сотрудник ЦРУ Томас Донахью заявил, что в ряде регионов за пределами США компьютерным злоумышленникам доступ к энергосетям открыт и по крайней мере однажды «это привело к отключению от электричества нескольких городов».

«Мы не знаем, кто организовал эти атаки и зачем, но во всех случаях имело место вторжение через интернет. Мы подозреваем, хотя утверждать не можем, что часть атакующих имела доступ к внутренней информации», – сказал сотрудник ЦРУ.

В последнее время эксперты, занимающиеся оценкой систем информационной безопасности, всячески пытаются привлечь внимание властей к слабым местам Системы диспетчерского контроля и сбора данных (*SCADA*). Она используется в важнейших элементах национальной инфраструктуры, начиная с электростанций и заканчивая дамбами и системой общественного транспорта.

По утверждениям директора по технологиям фирмы *BT Counterplane*, которая работает в сфере компьютерной безопасности, Брюса Шнайера, специалистам не следует полностью полагаться на слова Донахью и считать, что единственным слабым звеном в упомянутых им кибератаках была система *SCADA*. Если проникновение, как утверждает ЦРУ, было осуществлено с использованием «внутренней информации», то не исключена большая вероятность того, что его вполне могли организовать и сотрудники электростанций, имеющих права администраторского доступа в данную систему. Шнайер также заметил, что не стал бы «делать поспешных выводов» по поводу ненадежности ЭВМ, а подумал бы о надежности персонала.

Ради защиты Америки

Здесь стоит напомнить, что Белый дом давно добивается, чтобы спецслужбам США было предоставлено право без каких-либо судебных санкций прослушивать телефонные переговоры и перлюстрировать электронную почту иностранных граждан, находящихся за границами Соединенных Штатов, но использующих американские спутниковые каналы, узлы связи или интернет-серверы. Директор национальной разведки США Майкл Макконнелл как-то объявил, что это позволило бы «устранить значительный пробел» в предотвращении терактов на территории США, планы которых разрабатываются за пределами Америки. По его словам, требования на предварительное получение соответствующих судебных санкций существенно тормозит усилия спецслужб по оперативному вскрытию и срыву таких планов боевиков.

Вот почему 24 января, вскоре после подписания директив №54 и №23, Буш в очередной раз потребовал от Конгресса США сделать бессрочным закон, облегчающий слежку за иностранцами, подозреваемыми в терроризме и находящимися на территории других стран.

В распространенном заявлении хозяина Белого дома содержится напоминание, что срок действия временного Закона «О защите Америки» истекает 1 февраля. «Однако угроза со стороны «Аль-Каиды» не исчезнет через восемь дней. Действия Конгресса или его бездействие по этому важному вопросу напрямую отразятся на наших возможностях по обеспечению безопасности американцев», – подчеркнул Буш.

Закон, который после его подписания президентом получил название «О защите Америки», Конгресс принял в августе прошлого года под усиленным давлением Белого дома. Этим юридическим актом были внесены необходимые поправки в Закон «О контроле иностранных разведок», утвержденный еще в 1978г. Однако срок действия дополнительных полномочий АНБ, которое, обладая мощнейшими техническими средствами, постоянно слушает американцев, был ограничен шестью месяцами. Свое решение парламентарии объяснили тем, что они хотят принять более корректный, полностью обоснованный закон. Однако представители Демократической партии категорически возражали и против представленного в августе документа. Они неоднократно заявляли, что в процессе слежки могут быть нарушены права американцев, поскольку коренные жители США пользуются теми же узлами связи и серверами, что и граждане иностранных государств.

В ноябре прошлого года парламентарии проголосовали за поправку к Закону «О защите Америки» вопреки угрозам Буша, грозившего наложить свое вето. В результате АНБ все-таки обязали просить суды о разрешении на прослушивание телефонных переговоров в тех случаях, когда иностранец связывается с американским гражданином. Законодатели также отказались выполнить требование президента и о том, чтобы телефонные компании добровольно, без получения санкции судебных органов, оказывали АНБ содействие в слежке за жителями Америки и их зарубежными корреспондентами. Правда, республиканцам в Сенате удалось заблокировать инициативы своих демократических оппонентов...

Владимир Иванов

О РОЛИ СМЫСЛА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[1]

В ходе взаимодействия политических и социальных объектов на пути к своим целям, особенно когда эти цели связаны с доступом к жизненно важным, всегда ограниченным ресурсам, происходят неизбежные столкновения интересов, которые порождают соперничество (конкуренцию) и даже борьбу. Как показывает мировая история, разрешение меж- и внутригосударственных противоречий, имеющих характер антагонистических, традиционно осуществлялось и продолжает осуществляться в форме военных конфликтов различного масштаба.

Эти конфликты, как правило, сопровождаются вторжением агрессора на территорию государства-жертвы (племени-жертвы, этнической или религиозной группы-жертвы и т.п.), низложением правящей элиты, захватом столицы, уничтожением или присвоением победителями материальных, людских, территориальных и других ресурсов побежденных. И все это на фоне гибели массы людей и катастрофического материального ущерба для воюющих сторон.

В современных условиях наступление печальных последствий таких «разрешений противоречий» стало идти вразрез с экономическими интересами субъектов-хишников, а огласка последствий – и с их «розовым» (или «оранжевым») политико-демократическим имиджем. Тогда вновь приобрели актуальность былые достижения военно-теоретической мысли, допускающей возможность политической и экономической экспансии с помощью скрытых, непрямых действий, в которых человеческие жертвы и разрушения инфраструктуры не являются непременными.

Когда человечество в середине XX века вступило в постиндустриальный этап развития и последовал переход к информационному обществу, у агрессора *появилась* возможность решать свои стратегические задачи на межгосударственном уровне посредством специально организованных информационных воздействий на жертву.

Оказалось, что воздействия такого рода менее затратны даже в случае воплощения самых масштабных агрессивных устремлений. При этом государства (или социальные группы), не способные защититься от таких воздействий, обеспечить информационную безопасность, рискуют незаметно для себя утратить политическую, экономическую и любую другую самостоятельность. С этим в недалеком прошлом столкнулся Советский Союз, мировая система социализма, и на последнем этапе – субъекты постсоветского пространства. Общеизвестным стало еще одно понятие – «информационная война». В чем угроза такой войны и почему противодействие в такой войне представляет собой проблему?

После того как информационная безопасность была нормативно закреплена в качестве самостоятельной составляющей национальной безопасности нашего государства и утверждена Доктрина информационной безопасности Российской Федерации[2], в российских СМИ прочно заняли свое место понятия «информация», «информационная безопасность», «объекты обеспечения информационной безопасности». Только чем дальше мы продвигаемся по пути к информационному обществу, тем более эти понятия превращаются в подобия клише, которые при их частом употреблении стираются и перестают нести подобающую смысловую нагрузку.

---

[1] Военная мысль. Военно-теоретический журнал. N 11, ноябрь, 2007г.

[2] Федеральный закон «О безопасности» от 5 марта 1992 года.; Доктрина информационной безопасности Российской Федерации (утверждена поручением Президента Российской Федерации от 9 сентября 2000 года (приказ № 1895).

Хотелось бы поделиться соображениями, почему подобная «бессмысленность» сама по себе становится угрозой информационной безопасности и личности, и общества, и государства, особенно в контексте обеспечения военной безопасности.

На наш взгляд, упомянутые объекты обеспечения информационной безопасности – это объекты (процессы) материального мира, реализующие в себе функции получения, обработки, хранения и передачи информации, а также обладающие программами реализации этих функций.

К таким объектам относятся собственно информация (например, сообщение, фрагмент компьютерной программы, концепция, знание, мировоззренческая картина, информационный ресурс и т.п.) или ее носитель. Подобный носитель может быть как неодушевленным, техническим, так и одушевленным – социальным и социально-техническим (далее – социотехническим).

Все это приводит к мысли о создании универсальной модели объекта, анализ которой позволил бы сформировать системные характеристики объекта, выделить критически важные элементы для защиты от воздействия и в конце концов определить пути обеспечения его информационной безопасности.

Исходя из представленной схемы (рис. 1), элементами данной модели могут быть: системная структура объекта; ресурсы, которыми он обладает; программы, которые обеспечивают выполнение им функций и которыми обеспечивается управляемость со стороны субъекта; механизмы управления, посредством которых объект реализует свои функции.

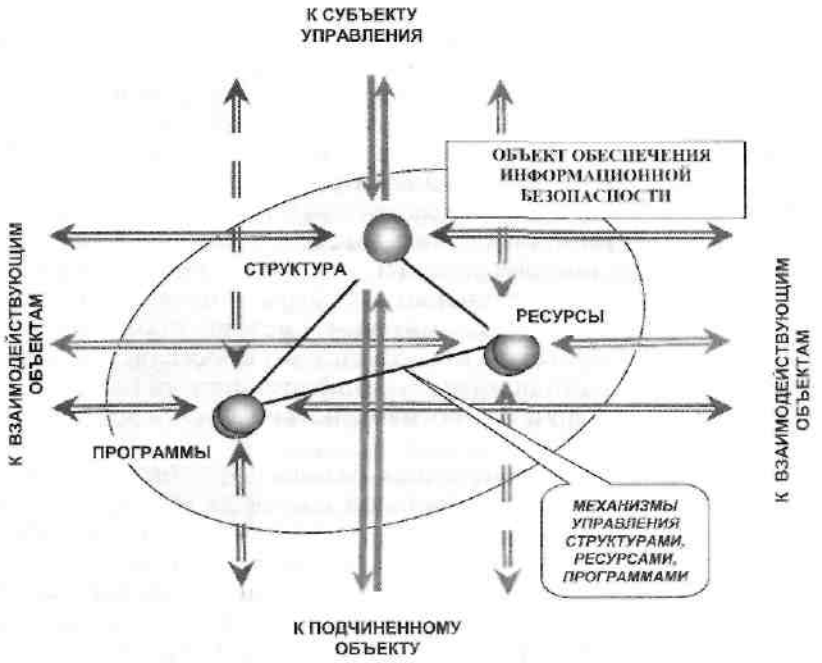


Рис. 1. Универсальная модель объекта обеспечения информационной *безопасности*

В данном случае структура объекта обеспечения информационной безопасности может быть представлена в виде информационной инфраструктуры, а также как комплекс других структур, например политической, экономической, организационной, социальной, биологической и др. (рис. 2).

Неотъемлемым элементом системы являются структурные связи. В данном случае представим их в виде элементов механизмов управления: административных, экономических, технологических, образовательных, обеспечивающих формирование общественного мнения и поддержание культурных и исторических традиций, архетипические (через бессознательное), пропагандистские, организационные и пр.

Рассуждения о механизмах управления следует дополнить тем, что предметом управленческой деятельности является формирование поведения (деятельности) объекта. При этом,

включая в себя субъект и объект управления как два противоположных полюса, деятельность обладает двусторонней чувствительностью к воздействиям и со стороны субъекта, и со стороны объекта, что отражается в наличии двух форм ее регуляции. Первая, предметная, связана с обеспечением соответствия деятельности объекта предмету (цели) деятельности и обстановке. Вторая, смысловая регуляция обеспечивает согласование целей и средств деятельности с мотивами, потребностями, ценностями и установками субъекта.

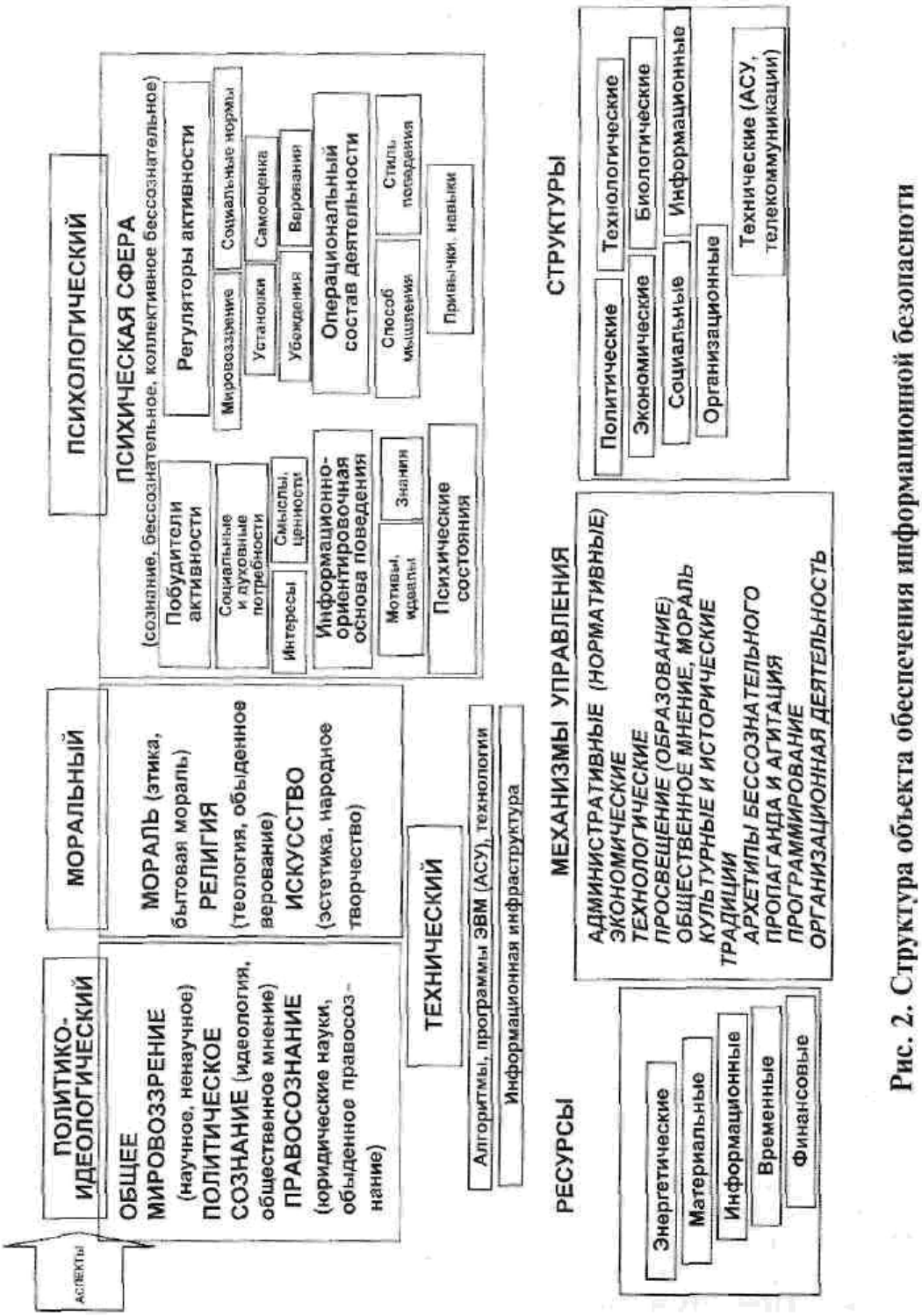


Рис. 2. Структура объекта обеспечения информационной безопасности

Далее, объект обеспечения информационной безопасности должен содержать некий ресурс, в первую очередь информационный, а также, возможно, какой-либо иной – энергетический, финансовый, пространственный, временной, материальный и пр.

Ключевой составляющей объектов обеспечения информационной безопасности являются программы, на которых, собственно, и базируются функции управления этими объектами. К таким программам с определенной степенью допущения могут быть отнесены: *политико-идеологические установки* – общее мировоззрение, политическое сознание (идеология, общественное мнение) и правосознание; *моральные обязательства* – нормы морали (этика, бытовая мораль), национальные традиции (духовные, культурные, исторические и т.д.), религиозные верования, принятые эстетические нормы; *психические программы* – побудители и регуляторы активности (социальные и духовные потребности, смыслы, ценности, интересы, самооценки, убеждения), принятый способ мышления, стиль поведения, привычки и навыки; *информационно-ориентировочная основа* поведения (мотивы, идеалы), предписанные для выполнения задачи, а также технические программы – алгоритмические, математические, технологические и пр.

В качестве центрального структурного образования системы управления сложным социотехническим объектом рассматривают конечную цель и смысл управления, определяемый как значимость для данной системы (объекта) того, что ведет к цели или способствует ее достижению.

В интересах дальнейшего рассуждения примем в качестве исходной одну из существующих формулировок понятия «информация» как результата отражения движения объектов материального мира в системе живой природы. При этом для человека информация отражает внешний мир в его сознании с помощью видимых, слышимых, ощущаемых знаков или сигналов.

Не вступая в противоречие с официальными трактовками[1], примем за основу, что информация фиксируется в общественном (массовом, групповом, индивидуальном) сознании, в частности воинских формирований, и (или) на материальных носителях (базах данных) их информационной инфраструктуры. Причем фиксация информации на материальных носителях в ходе управления войсками (силами) осуществляется в рамках служебной деятельности органов управления и отражается в сознании каждого должностного лица, принимающего решения. Допустим, что отображаемая таким образом информация называется сведениями, а отобранные, обработанные и проанализированные сведения называются данными.

Исходя из приведенного нормативного определения, утверждаем, что информация как совокупность сведений воспринимается сознанием человека. При этом каждый человек обладает определенным, свойственным только ему восприятием или информационной моделью мира[2], и получаемые сведения используются им для выбора рационального варианта социального поведения.

При накоплении сведений об окружающем мире в общественном сознании вырабатываются знания, а информационный ресурс накапливается в хранилищах информации (компьютерных базах данных, архивах, библиотеках).

Поскольку восприятие информации человеком основано на механизме «формирования внимания»[3], восприятие информации определяется как процесс ее соотнесения к некоторому уже известному классу и тем самым наделения ее смыслом. Иначе говоря, восприятие

---

[1] Информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. (См.: Доктрина информационной безопасности Российской Федерации, 2000г.).

[2] Модель мира — совокупность представлений о сущностях и процессах реального мира, приобретенных человеком в результате накопления и анализа индивидуального и социального опыта, активно использующаяся для выработки управленческих решений; модель фрагмента реальности, являющегося предметом мыслительной деятельности; модель субъекта, мыслимая им самими; модель инструментария сбора данных; модель источника сообщения. (См.: *Курносое Ю.В., Конотопов П.Ю.* Аналитика: методология, технология и организация информационно-аналитической работы. М.: Изд. «Русаки», 2004).

[3] *Дормашев Ю.Б., Романов В.Я.* Психология внимания: Учебник. М.: Московский психолого-социальный институт Флинта, 2002. С. 376.

информации – это процесс построения внутреннего представления образа в рамках информационной модели мира. Данный образ сохраняется в памяти человека, является субъективным и определяется динамично изменяющейся в процессе жизни системой ценностно-смысловых категорий как психологическим механизмом, осуществляющим познание.

Таким образом, информационная модель мира не безотносительна к потребностям, мотивам, установкам человека, а обслуживает его жизненные процессы, осуществляющие реализацию данных мотивов и установок. Принимая за аксиому наличие во внутреннем мире людей разнонаправленных мотивационных линий, следует предполагать наличие системы механизмов, выполняющих работу по соотнесению, упорядочению, иерархизации и перестройке мотивационно-ценностно-смысловой сферы личности[1]. Составляющие данной системы – присущие человеку и обществу устойчивые смыслы значимых объектов и явлений, а также личностные ценности, которые являются наряду с потребностями источниками этих смыслов.

Информация передается в процессе коммуникации (если не рассматривать особенности бессознательного ее приема-передачи между живыми организмами) в виде сообщений, информационная ценность которых заключается в новых для адресата сведениях.

В теории информации приняты несколько различных мер, определяющих свойства информации в интересах коммуникации, в частности синтаксическая, семантическая и прагматическая.

В качестве синтаксической меры информации используется ее количество. Уменьшение количества может привести к нарушению информационной безопасности (например, к уничтожению элементов базы данных или просто к недостаточной информированности), а увеличение – повышает неопределенность информации.

Принципиальное значение для наших дальнейших рассуждений имеет семантический уровень генерации информации, когда результаты преобразования (решения поисково-оптимизационных задач) содержат новые смысловые элементы, ориентированные на конкретный вид деятельности объекта.

На прагматическом уровне возникают зависимости между ценностно-смысловыми структурами и деятельностью личности и общества, рассогласование или намеренные деформации которых представляют системную угрозу информационной безопасности социотехнического объекта.

Информационно-содержательный аспект понятия «смысл» часто соотносится именно с содержательностью, информационной насыщенностью получаемых данных, причем важными факторами содержательности являются связность и упорядоченность.

Наиболее развернутым подходом к смыслу в аспекте объединения личной и социальной действительности является теория смыслов Ф.Феникса[2]. Из шести рассматриваемых им смысловых реальностей (символика, эмпирика, эстетика, синноэтика, этика и синоптика) для исследования проблем обеспечения информационной безопасности имеют принципиальное значение следующие: символика, которая включает в себя языковые и другие структуры, служащие для выражения в коммуникации любых *смыслов,* эмпирика, содержащая фактическое знание о действительности, и синоптика, объединяющая в единую перспективу смыслы, относящиеся ко всем остальным реальностям (в том числе областям знаний – по истории, религии, философии и пр.). Здесь смыслы выступают как предмет обучения, призванный обеспечить развитие смыслов и обеспечить их интеграцию в иерархическую структуру.

Таким образом, сведения как форма представления информации имеют: *во-первых,* факт своего объективного наличия, т. е. фиксацию момента создания (отправки и получения), способ представления (в устной, письменной, сигнальной форме и т. п.), стиль (литературный, обыденный), а также источник и категорию потребителя (образовательный статус, социальная или профессиональная группа и т. п.), факт коммуникации, способ взаимодействия (монолог,

---

[1] *Леонтьев Д.А.* Психология смысла: природа, строение и динамика смысловой реальности. М.: Смысл, 2003. С. 142.

[2] *Леонтьев Д.А.* Психология смысла: природа, строение и динамика смысловой реальности. М.: Смысл, 2003. С. 46.

диалог, интервью и т. д.), *во-вторых* – отражение в виде материальной формы знака (символа); *в-третьих*- свое предметное значение[1], *в-четвертых* – свое смысловое значение.

Для исследования проблем обеспечения информационной безопасности важен вывод основоположника экзистенциальной теории человеческого поведения Р.Мэя и его последователя Дж.Гинзбурга, исследовавших социокультурную детерминацию смыслов и утверждавших, что любое взаимопонимание основывается на совместной смысловой матрице участников коммуникации[2].

«Действия обладают смыслом, и для того чтобы взаимодействие сопровождалось пониманием, смыслы действий должны стать общими для участников взаимодействия... Процесс взаимодействия включает в себя активное формирование временной и, как правило, частичной общей для всех схемы социальной действительности. Формирование схемы может включать обмен смыслами между участниками взаимодействия ... как динамическое пересечение смыслов»[3].

Таким образом, смысл реализуется через контекстные условия обращения информации, в первую очередь зависящие от свойств источника сведений и его получателя. Корректировка субъектом одного из рассматриваемых параметров сообщения – факта, знака или содержания, а также контекста восприятия – изменяет смысл, по-другому воспринимаемый объектом.

Изменение ситуации, в которой осуществляется деятельность объекта, меняет смысл применения ранее заложенной в него программы (поставленной ему задачи), хотя алгоритм действий, предусмотренный той же программой, может остаться неизменным. Тогда принятие решения на продолжение следования прежней цели остается за исполнителем, который без дополнительной мотивации может произвольно откорректировать заложенную в него программу.

Если поставленная ранее задача заключалась во внутриситуативном действии, поведение объекта после изменения обстановки или завершения деятельности может стать неожиданным для субъекта, поскольку для объекта изменится (или будет утрачен) смысл его действий, и тот вынужден будет искать его в ином режиме или другой области деятельности.

Так, контрактные основания, принятые государством для поступления граждан на военную службу, могут обладать для последних иным смыслом по сравнению с призывом на военную службу в связи с его традиционным представлением в общественном сознании как формы исполнения священного долга перед Отечеством. Если военная служба является долгом, то смысл ее сохранится в любой ситуации и в критических условиях может реализоваться в жертвенности своей жизнью, здоровьем, интересами и т. п. Если же военная служба – средство достижения материальных благ, то в экстремальных условиях нельзя гарантированно рассчитывать на устойчивость морально-психологического состояния военнослужащего.

Таким образом, изучение значения сведений является лишь необходимым, но недостаточным условием обработки информации. Главное состоит в правильности извлечения вложенного смысла, от чего зависит не только достоверность информации, но и последующие действия объекта в соответствии с имеющейся программой (поставленной задачей).

Смысловым содержанием определяется основная ценность сведений, и смысл, будучи явным, скрытым или противоречивым, может придавать сведениям, имеющим одинаковое значение, пресловутую новизну, которая и является одним из базовых свойств информации.

Сообщения, закодированные или изложенные на неизвестном для получателя языке, могут не нести значения и смысла, но давать сведения о факте сообщения. Для другого получателя, посвященного в коды и языки, существует возможность получать информацию не только о факте, но и о значении, извлекать из них смыслы.

Одна и та же значимость в различных условиях порождает различный смысл. Отсюда следует, что смысл – это характер и мера значимости того, что ведет к цели, которая зависит от характера потребности и от условий ее удовлетворения. Смысл можно *понять* (увидеть связь и

---

[1] *Тульчинский Г.Л.* Текст как интонированное бытие или инорациональность семиотики // Философия языка и семиотика / Под ред. А.Н. Портнова. Иваново: Ивановский гос. ун-т, 1995. С. 44—52.

[2] Там же. С. 59.

[3] Там же. С. 74.

оценить значимость), согласившись или не согласившись с ним, а можно *принять,* т. е. решив действовать в соответствии с понятым. Не найти смысла значит не увидеть связи того, смысл чего мы ищем, с чем-то значимым. Следовательно, утрата смысла – это или утрата объектом определенной связи, или низкая оценка значимости того, о чем идет речь. Факторами, способствующими утрате смысла, могут быть распространение духа критицизма и скептицизма, деперсонализация и фрагментация жизни, обилие подлежащей усвоению культурной продукции и быстрый темп изменений условий жизни.

Функцию извлечения смысла может нести только психологический объект, и под извлеченным им смыслом следует понимать не только то, зачем определена та или иная цель его деятельности субъектом, но и идентификацию своего, объекта, отношения к данной цели.

Следует важный вывод: безопасность информации как объекта обеспечивается не только соблюдением традиционных требований ее *целостности, достоверности* и *конфиденциальности,* но и сохранением (скрытием) изначального *смысла, непротиворечивостью, недвусмысленностью* (или, напротив, противоречивостью и двусмысленностью!) *сообщений.*

В теории различается «порождение» смысла и «наделение» смыслом[1]. Смысл порождается значимостью цели, а наделение им того или иного действия происходит путем распространения этой значимости по ходу связей. При этом объекту, явлению, процессу, ситуации мы сначала придаем значение, а затем (и в результате этого) они обретают для нас смысл. Слабость распространения значимости цели на действия, ведущие к ее достижению, лишают эти действия смысла.

Второй аспект понятия «смысл» – личностный. Данный смысл может быть понимаемым и принимаемым. Понимаемый смысл – это категория, значимая для конкретных действий. Но смысл этого вида не имеет решающего значения при выборе направлений деятельности, его можно упустить без особого ущерба для личности.

Напротив, принимаемый смысл оказывает влияние на мотивационную сферу, изменяя характер отношения объектов к другим объектам, процессам, явлениям. Именно в ходе принятия смысла и накопления опыта его реализации индивид развивается как личность, накапливая жизненный опыт.

В течение своей жизни военнослужащий многократно оказывается в положении, когда необходимо найти смысл в поручаемом ему деле, т. е. в том, в чем ранее смысла для себя он не видел. При этом освоение любого нового вида деятельности, овладение новой специальностью, в частности военной, перемещение из одного места службы на другое связаны именно с нахождением в них смысла.

Если офицер думает только о трудности военной службы, значит, смысла в этой службе он не находит, а если, не обращая внимания на трудности, думает о том, какие возможности служба перед ним открывает, значит, он нашел в ней смысл. Успешное нахождение смысла дает ему энергию для деятельности и способность преодолевать жизненные препятствия. Развитая личность имеет склонность к перенесению тягот военной службы, ориентируясь на двойной ее результат: результат действий и самоутверждение посредством этой деятельности. Деятельность становится ценностью сама по себе, помимо конкретных ее результатов, поэтому служба при определенных условиях из просто обязанности (внешней необходимости) становится еще и внутренней необходимостью (потребностью).

Характерным для человека является то, что его потребности, привычки и интересы носят принципиально личностный характер. В силу уникальной интерпретации получаемой информации и создания своего образа мира для организации человеком своих отношений с миром вводится в качестве объяснительного понятия категория мифа – культурного и индивидуального. «Миф как принципиально иллюзорная точка отсчета, позволяющая человеку выбрать там, где привычные средства выбора не помогают... Именно миф расставляет перед человеком систему своеобразных «указателей»: что должно являться более ценным... значимым, а что –

[1] *Леонтьев Д.А.* Психология смысла: природа, строение и динамика смысловой реальности. 2 испр. изд. М.: Смысл, 2003. С. 46.

второстепенно. Именно миф создает систему... базовых ориентиров, которые позволяют представителю той или иной общности твердо знать, каким факторам окружающего предметного мира следует отдавать предпочтение»[1].

Считается, что основой присвоения смыслов «своей» социальной общности является общий миф: «Люди, погруженные в один и тот же миф, понимают друг друга с полуслова. Миф – это тайный язык смыслов, сама суть которого состоит в том, чтобы сделать данную культуру непроницаемой для представителей других культур»[2].

Будучи создан, миф становится основанием общей идентичности представителей данной социальной группы. Вопрос о правильности или истинности мифа не имеет значения: принимая и разделяя миф, объект тем самым ставит себя внутрь той культуры, социума, который сплочен именно этим мифом, а усомнившись в нем, просто оказывается в позиции чужого по отношению к ней. «Смысл есть высшее знание не потому, что он несет в себе объективную истину, а потому, что он несет в себе знак принадлежности той или иной культуре»[3].

В качестве примера системы мифотворчества следует предложить феномен веры как центральной мировоззренческой позиции и психологической установки, включающей произвольное принятие определенных установок и решимость их придерживаться. Следование вере, как показывает история развития социальных отношений, позволяет формировать и хранить в сознании модель мира, включающую в себя все необходимые для личности смыслы и ценности, даже если для этого нет объективных причин, тем более что выделение в жизненном мире субъекта ведущих смысловых ориентиров ведет к образованию оснований поведения (жизнедеятельности), а разрушение данных ориентиров – к лишению поведения рациональных оснований.

Исходя из вышеизложенного, следует допустить, что информационная безопасность объекта зависит от его способности в процессе жизнедеятельности вкладывать, извлекать, хранить смыслы и оперировать ими, управляя при этом смыслами деятельности подчиненных объектов.

Приведенные рассуждения совсем по-другому высвечивают представления об информационной безопасности личности, общества, государства и проблемах ее обеспечения. Постановка вопроса подобным образом позволяет еще на уровне понятий обозначить ядро проблем, связанных с угрозами общественному сознанию, в котором смыслы – не только мишени, но и средства информационного воздействия, а также ключи к пониманию действительности.

В этом случае к известным требованиям к информации необходимы дополнения, касающиеся непосредственно информационной безопасности объекта, в частности наличия в информации, направляемой объекту, согласующегося с функциями данного объекта и его картиной мира смысла, который должен быть в зависимости от целей подачи информации скрыт от непосвященных. Такое добавление является принципиальным и имеет методологическое значение. Назовем данное требование к информации, например, смыслообусловленностью

Данный вывод имеет существенное значение для обеспечения информационной безопасности войск (сил) и устойчивости военного управления (психологические аспекты), которые базируются на формировании смыслов деятельности лиц, принимающих решения, и личного состава органов управления и войск (сил).

Рассмотренные в данной статье вопросы призваны привлечь внимание читателя к необходимости осмысления своей роли и места в военном деле нашего государства, послужить толчком к возведению в своем сознании преграды на пути изощренных информационных воздействий, посредством которых нашему Отечеству может быть нанесен непоправимый ущерб.

Дербин Е.Л.[4]

---

[1] *Лобок А.М.* Антропология мифа. Екатеринбург. 1997. С. 56—57.

[2] *Лобок А.М.* Антропология мифа. Екатеринбург. 1997. С. 21.

[3] Там же. С. 86.

[4] Генерал-майор, кандидат военных наук, доцент, начальник кафедры информационной безопасности Военной академии Генерального штаба Вооруженных Сил Российской Федерации.

СИСТЕМА СИСТЕМ:
ИНФОРМАЦИОННО-УДАРНОЕ ОРУЖИЕ[1]

Человечество на рубеже тысячелетий одновременно с вступлением в эпоху новой информационно-космической цивилизации [1, 2] вступает в эпоху войн шестого поколения с широким задействованием в ходе их подготовки и ведения всего разнообразия космических средств.

Свидетельством тому является появление целого ряда теоретических разработок [3], посвященных обоснованию концептуальных положений по подготовке и ведению асимметричных, бесконтактных, сетевых, нелетальных, *управляемых* информационных войн и войн в киберсфере.

В войнах нового поколения [4] решающая роль будет отводиться уже не существующему стратегическому ядерному оружию, и даже не живой силе, а высокоточному оружию *в микроядерном (оружие империи XXI столетия!)* и обычном оснащении и оружию, построенному на новых физических принципах.

Политические перемены последнего времени оказали влияние на процессы сокращения наступательных и оборонительных вооружений, предопределили необходимость пересмотра основных военно-доктринальных установок и реформирования структур вооруженных сил ведущих государств мира. Причем вопрос в данном контексте с учетом рассматриваемых тенденций и особенностей развития человечества ставится следующим образом: обеспечить реализацию требуемых боевых возможностей вооруженных сил, соответствующих национальным интересам того **или** иного государства за счет меньшего количества войск, но лучшего качества оружия и лучшего качества личного состава.

Знание – сила

Необходимо учитывать, что одной из важнейших особенностей развития человеческой цивилизации в XXIв. является превращение наукоемкого продукта в определяющий фактор экономического развития и главный источник пополнения бюджета государств. Влияние этой особенности на область военной деятельности определяется начавшейся *новой революцией в военном деле,* основой которой станут научно-технические достижения, способные преобразить вооруженные силы развитых стран и способы ведения ими боевых действий, а также изменить соотношение сил в мире.

В условиях, когда во многих странах мира идет практически непрерывное развитие и переоснащение вооруженных сил, когда принимаются долгосрочные программы разработки и создания новых видов оружия и военной техники, значительную важность приобретают прогностические оценки характера вооруженной борьбы будущего.

При этом развитие военного дела на пороге третьего тысячелетия, как показал анализ, будет определяться рядом ведущих мировых тенденций, которые основываются на следующих четырех положениях [5]:

- Процесс интенсивного внедрения современных информационных технологий в военную сферу привел к существенному ускорению процесса перевооружения армий ведущих государств мира с ударных на информационно-ударные системы I оружия.
- Наиболее интенсивно этот процесс происходит у государств, которые имеют хорошо развитую космическую инфраструктуру (США, Россия, Франция, Китай, Япония, Индия) и способны оперативно наращивать информационную мощь в космосе.

[1] Индекс безопасности. Российский журнал о международной безопасности. N 3 (83), 2007г.

- Появляются и натурно отрабатываются новые оперативно-тактические концепции применения перспективных вооруженных сил, обеспечивающие посредством космоса, информации и оружия достижение глобального информационно-ударного превосходства.
- Происходит существенное возрастание зависимости эффективности военных действий в традиционных сферах – суша, воздух, море – от действий в космосе. Развивается процесс целенаправленного переноса потенциала угрозы в космос.

В ходе проведенных исследований было определено то общее и новое, что объединяет эти разноплановые тенденции – это превращение информации в новую составляющую вооруженной борьбы. Действие этого явления в военном деле проявляется в двух, как представляется, самостоятельных областях.

Первая – область информационного противоборства. Она охватывает вопросы поражения информационного ресурса противоборствующей стороны и защиты собственного информационного ресурса при помощи средств информационной борьбы. Действие процессов в этой области приводит к созданию систем информационного оружия.

Вторая область – информационно-интеграционная. Она охватывает вопросы сопряжения информационных разведывательных, связных, навигационных и других систем с существующими ударными средствами.

Информационно-ударная система оружия

Для характеристики систем оружия, создаваемых на основе интеграции информационных и ударных средств и отличающихся повышенными боевыми свойствами и возможностями, было обосновано и *введено новое собирательное понятие – информационно-ударная система оружия*[1] *(ИУСО).*

На основе создания многослойных информационно-управляющих полей в указанных системах оружия достигаются заданные параметры слежение за объектами поражения с высокоточной выдачей целеуказаний и контролем результатов воздействия; формируется единая координатно-скоростная и временная основа для согласованного применения всех элементов ИУСО; реализуется непрерывный внутрисистемный обмен всеми видами информации и многоконтурное управление, обеспечивающее требуемую периодичность доведения данных при подготовке и нанесении ударов до пунктов управления, носителей средств поражения и ударных средств на всех участках полета к цели.

Это позволяет получить в ИУСО такое *новое качество наведения,* которое наряду с достижением массированности наносимых ударов *обеспечивает поражение целей (прежде всего мобильных) с первого выстрела или пуска с вероятностью не ниже 0,9.*

В свою очередь, реализация информационно-интеграционной идеи приводит к замене чисто ударных средств вооруженной борьбы на целый класс ИУСО тактического, оперативно-тактического, стратегического уровней и знаменует собой завершение этапа создания систем

---

[1] Под информационно-ударными системами оружия будем понимать системы и комплексы оружия, включающие в свой состав информационные (разведки, связи и ретрансляции данных, навигации), управляющие, ударные и обеспечивающие компоненты различного базирования, способные формировать пространственно-временные (согласованные с планируемыми параметрами удара) многослойные информационно-управляющие и боевые поля, определяющие качественно новые оперативные и боевые возможности ИУСО. Указанные ИУСО отличаются от известных систем высокоточного оружия тем, что в них командно-управляющая информация, циркулирующая в рамках системы, замыкается не только на носитель, а, прежде всего, на средства поражения на всех участках их полета к цели. В результате этого ИУСО реализует уже не концепцию «выстрел-поражение» ($P_{пор}>0,5$), а концепцию оружия *прецизионного наведения* ($P_{пор}>0,9$).

высокоточного оружия и переход к новому качественному этапу создания систем оружия *прецизионного наведения.*

При реализации этих систем оружия делается ставка на достижение возможности поражения не только стационарного защищенного, но и мобильного объекта, в том числе и на межконтинентальной дальности, с одного выстрела (пуска) за счет прямого попадания в цель[1].

Представляется, что структура гипотетического состава разноуровневых ИУСО будет носить пирамидальный характер *(Рисунок 1).* Это обусловливает значительное увеличение типажа ИУСО при перемещении от вершины к основанию пирамиды (на оперативно-тактический и тактический уровни).

Рисунок 1

Структура разноуровневых ИУСО [8]

Для переноса этих идей с тактического на оперативный и стратегический уровни начался поиск универсальных информационных технологий и систем, обеспечивающих их реализацию. Такими системами оказались информационные космические системы (ИКС), но разрабатываемые уже не по существующим технологиям крупногабаритных космических аппаратов (КА), а по перспективным технологиям малогабаритных КА и нанотехнологиям. Эти системы превращаются в умножитель возможностей ударных подсистем.

---

[1] Таким образом, для ведения войн шестого поколения требуется создание принципиально новой материальной базы, которая будет базироваться теперь уже не на чисто ударной, а на информационно-ударной техносфере. Основу информационно-ударной техносферы будут составлять информационно-ударные системы оружия, имеющие одинаковую структуру, одинаковые принципы построения, одинаковые принципы применения, но различные масштабы применения. Простейшие расчеты показывают, что по сравнению с системами высокоточного оружия с вероятностью поражения объекта с одного выстрела (пуска) $P_{пор} > 0{,}5$ в системах оружия *прецизионного на ведения* $P_{пор} > 0{,}9$ экономия может составлять 3-4 боеприпаса на каждый объект.

По мере интеграции ИКС в контур боевого управления ядерным оружием (ЯО) начинает неизбежно действовать закономерный этап вытеснения информацией из процесса вооруженной борьбы ЯО со значительными тротиловыми эквивалентами (q=100...600 кт), приводя к *его замене на* микроядерное оружие *реального применения* (q=0,01...0,05 кт).

В ходе практической реализации информационно-интеграционных мероприятий при создании ИУСО в общей классификации космических систем (КС) обозначился новый классификационный параметр – космические системы, включаемые в контур боевого управления (БУ) оружием *(Рисунок 1).* Одновременно пунктирно обозначились контуры совершенно нового явления – нарастающей степени интеграции разноплановых ИУСО по уровню решаемых задач и по функциональному предназначению в *систему систем* оружия. Именно подобные системы оружия способны существенно изменить облик вооруженных сил, всей военной организации *государства* и характер вооруженной борьбы, а также определить направления военной модернизации.

Анализируя указанные явления с позиций синергетики как науки об эволюции очень больших, сверхсложных систем, можно сделать вывод, что системообразующим, интегрирующим и системопреобразующим базисом при создании и насыщении войск перспективными системами оружия, вызывающими кардинальные изменения характера вооруженной борьбы, выступает совокупность разноплановых информационных (в том числе и космических) систем.

Интегрированные вооружения

Вместе с тем, чтобы перейти в новое качество и достичь готовности для включения ИКС разведки, связи и ретрансляции данных, навигации в контур боевого управления средствами поражения ИУСО различного уровня и функционального предназначения, должен быть выполнен ряд следующих требований:

1. Наличие применительно к каждой ИУСО как самостоятельного элемента оперативного построения или боевого порядка войск (независимо от уровня решаемых задач и предназначения) на постоянной основе средств наземного комплекса управления (НКУ) и наземного специального комплекса (НСК) для управления КА, получения и обработки космической информации, а также орбитальных группировок (ОГ) КА, не превышающих по численности некоторых пороговых значений количества объектов поражения ($N_{\text{nopp}i}$, $N_{\text{nopc}i}$, $N_{\text{nopH}}j$), определяющих нижний уровень реализации системой оружия системных свойств;
2. Обеспечение возможности оперативного наращивания состава ОГ каждой из ИУСО путем проведения запусков КА или передачи в оперативное подчинение такого количества орбитальных элементов, которое позволит превысить $N_{\text{nopp}i}$, $N_{\text{n0pc}j}$, $N_{\text{nopH}i}$ и реализовать в ИУСО в полном объеме системные свойства;
3. Развертывание принципиально новых орбитальных группировок, которые применительно к каждой из ИКС разноплановых ИУСО должны строиться в соответствии с двумя закономерностями:
   - обеспечения двухкомпонентного состава ОГ с наличием дежурного орбитального эшелона, развертываемого на основе крупногабаритных КА, и эшелона оперативного развертывания, создаваемого на базе малогабаритных КА;
   - ОГ каждой из ИКС должны быть многоспутниковыми, многоплоскостными и эшелонированными по высоте, увязанными в многофункциональную сеть разведки, связи и управления, интегрированную с системами оружия.

Помимо этого, необходимо учитывать, что ОГ каждой из ИКС, включаемых в контур БУ средствами поражения ИУСО, должны быть построены минимум в три эшелона и не случайно с учетом указанных особенностей в течение ближайших десяти лет предусматривается дополнительно развернуть более 1800 американских КА. Вместе с тем использование для этих

целей только КА военного назначения может оказаться нецелесообразным по экономическим и международно-правовым причинам.

Поэтому в качестве другого, альтернативного подхода может быть использован подход, основанный на совместном применении ресурса ИКС военного (двойного), социально-экономического и коммерческого назначения. Возможность совместного использования указанных систем при значительном положительном эффекте была неоднократно продемонстрирована в ходе локальных войн и вооруженных конфликтов конца XX и начала XXIвв.

Космос перестает быть мирным

Вследствие этого в число новых функциональных концепций применения космических сил США *(Рисунок 2)* наряду с такими концепциями, как *контроль космоса, глобальное применение силы, полная интеграция вооруженных сил,* была включена концепция глобальное *партнерство* [9]. Эта концепция предусматривает увеличение возможностей военного использования космоса путем объединения усилий гражданских, коммерческих, научных и международных КС.

Рисунок 2

Применение космических сил США

Указанные факторы обусловили возрастание темпов процесса целенаправленного переноса потенциала угрозы в космос. Этот процесс реализуется по двум направлениям: *опосредованно* за счет наращивания информационной мощи в космосе и включения основных КС разведки, связи и ретрансляции данных, навигации в контур боевого управления оружием и средствами поражения и *непосредственно* за счет развертывания в стратегической космической зоне (СКЗ) боевых космических средств (БКСр). Причем возможности реализации второго из рассматриваемых направлений находятся в существенной зависимости от первого из направлений, являющегося базовым.

Сегодня все ведущие страны мира с учетом рассмотренных тенденций пришли к пониманию своих геополитических интересов в космосе и развернули широкомасштабную косми-

ческую деятельность. Без космической деятельности сейчас уже немыслимо экономическое и социальное развитие государств [10].

О масштабах развернувшегося процесса свидетельствует тот факт, что порядка 40 государств работают над программами по использованию результатов применения космических средств в системах оружия, около 30 имеют государственные космические программы, 19 стран обладают производственной и научной базой, позволяющей им разрабатывать и производить собственные КА [11]. Однако развитой космической инфраструктурой, позволяющей самостоятельно решать сложные задачи освоения и практического использования космоса, наряду с Россией обладают лишь США, Франция, Китай, Япония и Индия.

Мировой спутниковый парк насчитывает более 700 КА при многомиллиардной стоимости. Значительная часть из общей численности орбитальных средств являются КА военного назначения. Более тысячи компаний мира напрямую связаны с космической индустрией.

К настоящему времени ассигнования на решение проблем военного использования космоса достигли очень высокого уровня. Общие ежегодные затраты США в этой области превышают $21 млрд. Причем около 20% из них приходится на спутниковые системы разведки.

Американские специалисты, оценивая общую картину запуска КА на околоземные орбиты, производят пересмотр прогнозов «Стратегического плана космических командований США до 2020г.» и отмечают, что в ближайшем десятилетии (до 2010г.) предстоит вывести в космос около 2200 полезных нагрузок, а не 1800, как планировалось ранее (на период до 2020г.).

В связи с этим возникает вопрос: насколько соответствует развернувшийся процесс создания ИУСО с использованием космических средств интересам мирового сообщества? Видимо целесообразно, чтобы этот вопрос решался путем международно-правового регулирования.

Вместе с тем решение сформулированной проблемы на рубеже XX и XXI вв. будет связано со значительными трудностями. Они связаны с переходом к структуре *монополярного миропорядка,* снижению роли ООН и обеспечению решения стратегических задач США и их партнерами посредством экономической и военной мощи. Налицо стремление к пересмотру в одностороннем порядке важнейших международных договоров и переносу центра тяжести в развитии вооружений в область космоса, что может иметь катастрофические последствия для судеб мира.

В настоящее время начала вырисовываться перспективная структура ВС США, формируемая на основе сопряжения информационных и ударных сил применительно к различным сферам вооруженной борьбы с широким задействованием в их составе космических сил и средств. Это обусловило необходимость разработки в США новых концепций применения перспективных вооружений и взглядов на ведение войны на период вплоть до 2020г., что нашло отражение в следующих основополагающих исследованиях и документах: «Космический прогноз-2020», «Единая перспектива-2010», «Стратегический план космических командований США до 2020г.», директива МО США 3100.10 от 9 августа 1999г., «Космическая политика», «Война в 2020г.» и др.

Анализ содержания части указанных документов показывает: в общей своей совокупности они определяют направленность работ, проводимых в США по превращению околоземного космического пространства в новую сферу вооруженной борьбы и достижению всеохватывающего превосходства[1]. Космос, по проводимым оценкам, стал национальной космической отраслью, которую необходимо защитить.

При этом:

- в «Космическом прогнозе-2020» определены технические аспекты реализации оператив-

[1] Необходимо отметить, что существующие тенденции развития форм и способов ведения вооруженной борьбы в ходе конфликтов различной степени интенсивности свидетельствуют о возрастании значимости задач глубокого неядерного поражения противника на всю глубину построения его войск с высокой оперативностью. Это определяет необходимость создания таких систем оружия, которые позволяли бы быстро реагировать на складывающуюся обстановку, осуществлять оптимальный выбор средств поражения для воздействия на объекты различного класса, а также имели бы высокую готовность к применению в любых условиях обстановки.

но-стратегических концепций повышения эффективности стратегического использования вооруженных сил на основе достижения превосходства в космосе: глобальный размах, глобальное присутствие, глобальная мощь;

- в «Единой перспективе-2010» отражены новые оперативно-стратегические концепции достижения всеохватывающего превосходства на основе реализации концепций: превосходства в информационной сфере, господствующего маневра, высокоточного сражения (боя), всеобъемлющей защиты, целенаправленного тылового обеспечения;
- в «Стратегическом плане космических командований США до 2020г.» приведены концепции достижения космического превосходства в XXIв.: контроль космоса, глобальное применение силы, полная интеграция вооруженных сил, глобальное партнерство, а также произведена их взаимоувязка с концепциями достижения всеохватывающего превосходства.

Система систем

Важнейшей особенностью изменения содержания вооруженной борьбы будет являться то, что в развитии средств ее ведения наступает эпоха новой техносферы – информационно-ударной. Материальным выражением этой техносферы является оружие межвидового уровня, создаваемое на основе комплексной интеграции средств разведки, связи и управления, навигации, радиоэлектронной борьбы и ударно-огневых средств в единые системы оружия стратегического, оперативного и тактического уровней.

С появлением технологии малогабаритных КА ярко выражена тенденция объединения разноуровневых ИУСО в *систему систем* оружия с присущими ей функциональными свойствами, такими как интеллект, организованность, управляемость, наблюдаемость, скрытность, боевая устойчивость, повышенные боевые возможности и др.

Система систем оружия обладает инвариантностью структуры по отношению к любому виду оружия за счет использования общей глобальной сети разведки, связи и управления, навигации, развертываемой в ближней и дальней стратегической космической зоне. Это придает системе свойства универсальности по отношению к масштабам применения, в том числе к объектам поражения различного базирования при скачкообразном повышении эффективности наносимых ударов.

Таким образом, теснейшая увязка информационных систем с ударными превращает их из средств опосредованного в средства непосредственного воздействия на объекты поражения. Указанная важнейшая особенность приводит к изменению метрики военных действий и окончательному формированию пятой – информационной составляющей вооруженной борьбы.

С созданием подобных систем оружия США приступили к реализации концепции сдерживания с применением неядерного оружия, обеспечивающей достижение целей войны без вторжения крупных группировок войск и захвата территории противника при минимальном экологическом ущербе.

Тем самым формируются условия по приданию неядерному оружию стратегической значимости и его превращению в эффективное средство ведения *противоскоростной* борьбы, нацеленной на гарантированное опережение противника во всех фазах вооруженного конфликта.

В связи с этим необходимо отметить, что в настоящее время в США осуществляется наращивание возможностей космических систем, реализующих информационную мощь в космосе и обеспечивающих проведение интегрирования *в систему систем* оружия теперь уже и БКСр. Это позволит напрямую сформировать потенциал угрозы в космосе и приступить к формированию принципиально новой всесферной системы оружия.

Данный процесс характеризуется рядом закономерностей:

- ускорение информатизации мирового сообщества посредством полного задействования ресурсов и возможностей космического пространства;
- возрастание лидирующего влияния космической техносферы на процесс превращения информации в новый предмет вооруженной борьбы;

- увеличение темпов реализуемости через космос разноуровневых информационно-ударных систем оружия с общими принципами построения.

Учет этих закономерностей, а также того, что космос является такой же средой, как суша, море или воздух, в которой будут осуществляться военные операции в интересах обеспечения национальной безопасности США, уже сейчас привел к формированию предпосылок к созданию пока еще не выделенного четвертого вида вооруженных сил США[1].

Угрозы безопасности

Все это приводит к возникновению потенциально новых угроз национальной безопасности Российской Федерации в военной области, основными из которых являются:

- отставание в темпах сопряжения информационных космических и ударных средств;
- угроза навязывания неадекватных темпов сокращения ударных группировок стратегических сил сдерживания и увеличение отставания по качественным параметрам от подобной группировки противника;
- возникновение угрозы навязывания неприемлемых условий и темпов переоснащения ракет стратегических сил сдерживания на головных частях (боевых блоках) с пониженным тротиловым эквивалентом;
- угроза обеспечения через космос возможностей по слежению за степенью готовности группировок стратегических сил сдерживания к применению и достижения эффекта *остационаривания* мобильных носителей средств поражения;
- придание всем существующим стратегическим ядерным средствам противника возможностей по поражению стратегических мобильных объектов;
- реализация концепции сдерживания с применением неядерного оружия за счет придания ему стратегической значимости и превращения в эффективное средство ведения *противоскоростной* борьбы, нацеленной на гарантированное поражение противника во всех фазах вооруженного конфликта.

Анализ вариантов структур и способов применения интегрированных боевых систем различных уровней показывает, что в условиях сокращения ударного компонента только за счет адекватного наращивания информационных возможностей космического компонента возможно решение задач сдерживания противника с заданным качеством.

Проведенный анализ позволяет выявить ряд факторов, влияющих на стратегическую стабильность:

- выделение из общего спектра КС ряда ИКС, которые по своим количественным и качественным параметрам превращаются в целостные функциональные подсистемы перспективных систем оружия;
- превышение пороговых значений количества КА в информационных ОГ КС разведки, связи и навигации, в том числе и однотипных коммерческих систем, включаемых в контур БУ оружием как по отдельности, так и совместно;
- превышение пороговых значений количества ударных средств различных сфер вооруженной борьбы, сопряженных с ИКС, обеспечивает скачкообразное приобретение той или иной стороной односторонних преимуществ и создание условий для решения стратегических задач без применения ЯО.

---

[1] Его формирование будет производиться в рамках не завуалированной и явно просматривающейся структуры – космических сил с четко определенным составом решаемых задач. Так, директивой Министерства обороны США 3100.10 от 9 августа 1999г. «Космическая политика» для главнокомандующего Объединенным космическим командованием (ОКК) определено, что он координирует и осуществляет планирование космической кампании в процессе общего планирования применения вооруженных сил в соответствии с национальной военной стратегией.

Это еще раз подтверждает тот факт, что космос и КС становятся не только важными и значимыми в ходе подготовки и ведения военных действий, но приобретают и выполняют важнейшую системообразующую роль, в том числе и при создании перспективных средств вооруженной борьбы.

Указанные особенности формирования потенциала угрозы в космическом пространстве позволяют сделать ряд выводов:

- Стремление к монопольному господству в космосе может составить один из основных аспектов реализации национальных военных стратегий отдельных государств. В результате в космическом пространстве может установиться национальный суверенитет, что не позволит другим странам осваивать и использовать преимущества этого пространства.
- Не исключается возможность создания ведущими странами мира новых систем космических вооружений.
- Для обеспечения военных действий на Земле расширяется использование коммерческих и гражданских спутниковых систем связи, телекоммуникации и дистанционного зондирования Земли, что приводит к объективной необходимости международно-правового регулирования этого процесса.
- Возникает опасность смещения центра тяжести в планировании использования космического пространства в интересах национальной безопасности с обеспечивающих (информационных) функций на чисто боевые.
- Без принятия дополнительных международно-правововых документов космическое пространство в перспективе может выделиться в самостоятельную сферу подготовки и ведения военных операций.

Космическое право

Изложенные тенденции с особой остротой ставят вопрос о регулировании использования космического пространства на базе норм международного права, в основу которого положен основной принцип: *что не запрещено – то разрешено.* Учитывая это обстоятельство, военно-космическая деятельность была условно разделена на три категории: разрешенную (оговоренную), запрещенную и неоговоренную международным правом. В рассматриваемом контексте и в связи с особенностями формирования потенциала угрозы в космосе наибольшую сложность при решении проблемы международно-правового регулирования представляют виды космической деятельности, которые не оговорены международным правом. К ним могут быть отнесены такие виды военно-космической деятельности, как проведение военно-прикладных космических экспериментов, в том числе связанных с отработкой технологии наведения средств поражения из космоса; создание и развертывание в космосе средств оптико-электронного и радиоэлектронного подавления; создание, испытание и развертывание ударных средств, которые могут поражать объекты в космосе и из космоса.

При решении проблем по ослаблению угроз национальной безопасности России в военной области необходимо учитывать возрастание лидирующего влияния результатов освоения космического пространства на превращение информации в новую составляющую вооруженной борьбы и, как следствие, – возможность создания перспективных систем оружия посредством сопряжения ИКС со всем существующим спектром средств поражения [14].

Основой для таких преобразований является то, что ряд КС по своим качественным и количественным параметрам или уже достигли, или в ближайшее время достигнут готовности для включения в контур боевого управления оружием. Поэтому в общей классификации КС появляется новый классификационный параметр – ИКС как функциональные подсистемы перспективных систем оружия [15]. Значит, можно предположить, что фактически любое средство поражения, наводимое на объект через космос, получает способность решения стратегических задач. Таким образом, появляется возможность выборочного поражения элементов инф-

раструктуры противника без площадного поражения территории и массовой гибели населения. Процесс создания вышеуказанных систем оружия необходимо рассматривать в трех аспектах:

- Новое качество решения разведывательных задач из космоса начинает обеспечиваться при повышении количественных параметров ОГ КА определенного порогового значения. При увеличении количества КА в ОГ разведки до 100-150 КА и выше *(График 1)* данная КС приобретает свойства инвариантности по отношению к разведываемым объектам, обеспечивая псевдореальный режим слежения за мобильными целями [16]. При обеспечении превышения количественных характеристик ОГ КС связи и навигации соответствующих пороговых значений все три рассматриваемые ИКС автоматически превращаются в развернутые подсистемы ИУСО, что является серьезным дестабилизирующим фактором.
- При сопряжении ИКС со всем существующим спектром средств поражения на основе достижения ими готовности для включения в контур БУ оружием эти системы из средств опосредованного воздействия по объектам поражения превращаются в средства прямого воздействия на разнообразные цели.
- Развертывание космической информационной инфраструктуры обладает свойством инвариантности по отношению к разнотипным средствам поражения, а следовательно, создаются предпосылки для развертывания в СКЗ и боевых космических систем.

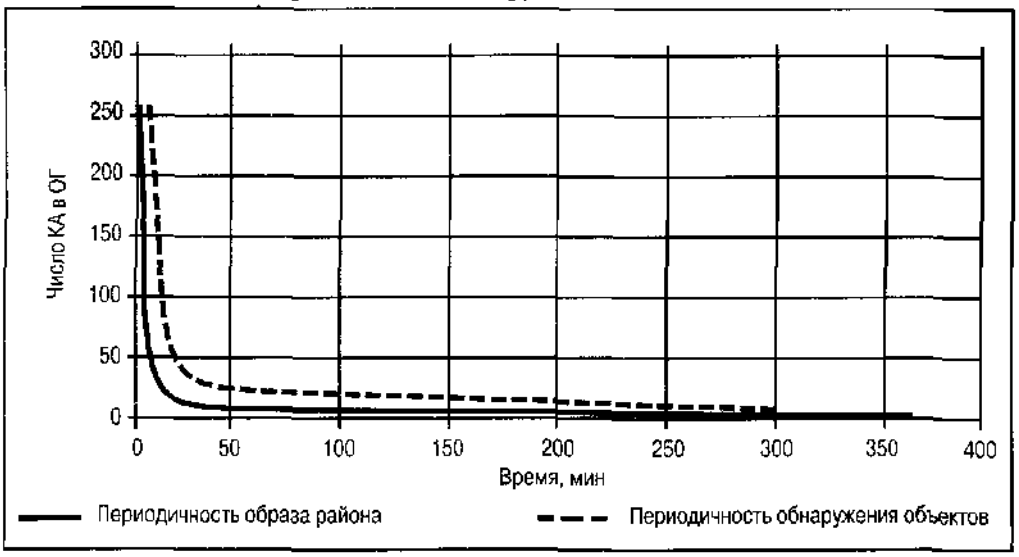
ОГ общего назначения, функционирующая в интересах военно-политического руководства государства, позволяет обеспечить этому государству глобальное превосходство над другими странами, как в космосе, так и на суше, в воздухе и на море.

В связи с этим возникает вопрос: насколько соответствует развернувшийся процесс создания ИУСО с использованием космических средств интересам мирового сообщества?

Целесообразно, чтобы этот вопрос решался путем международно-правового регулирования. Проблема заключается, однако, в том, что вышеперечисленные системы практически не определяются существующим международно-правовым ограничительным режимом космических вооружений. Очевидно, что без принятия дополнительных международно-правовых документов космическое пространство в перспективе может выделиться в самостоятельную сферу подготовки и ведения военных операций. Особенно важно то, что новая инфраструктура в области космоса и систем управления, связи и разведки является фундаментом для преобразования вооруженных сил и основанием, на котором они стоят.

График 1

Возможности ОГ систем радиолокационной разведки по периодичности обнаружения объектов [17]



Противоракетная оборона США

Ярким примером возможности достижения глобального информационно-ударного превосходства в скором времени может послужить Национальная система противоракетной обороны (НПРО) США.

Рисунок 3

Структура системы систем оружия [18]

Представляется, что данная система при ее окончательном развертывании превратится в *систему систем* оружия *(Рисунок 3),* способную в соответствии с замыслом решать две взаимосвязанные задачи: 1) эффективного слежения и последующего поражения всего спектра носителей тактических, оперативно-тактических и стратегических баллистических средств ведения вооруженной борьбы до проведения ими пусков; 2) поражения стартовавших баллистических средств, ушедших из-под удара, на всех участках полета к цели [19].

В структуру НПРО США на первоначальном этапе ее развертывания будут входить: КС обнаружения пусков баллистических ракет; КС сопровождения космических и баллистических целей; обновленные радиолокационные станции (РЛС) раннего предупреждения о ракетном нападении; ракеты-перехватчики наземного базирования; станции связи с перехватчиком в полете; центральный пункт командования, управления и связи.

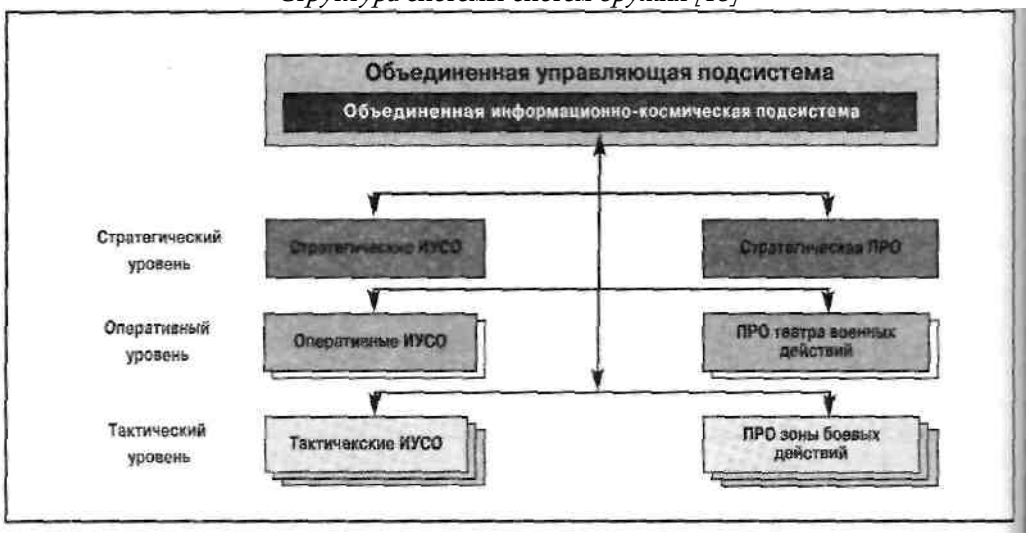
Наибольший интерес в рассматриваемом контексте имеет информационная подсистема НПРО США, в состав которой будут входить: КС начального обнаружения пуска межконтинентальных баллистических ракет (МБР) и слежения с шестью КА на стационарной и высокоэллиптической орбитах; низкоорбитальная КС сопровождения МБР и баллистических ракет на подводных лодках (БРПЛ) в полете в составе 24 КА; пять усовершенствованных РЛС дальнего обнаружения, работающих в сантиметровом диапазоне длинных волн; до девяти *РЛС* Х-диапазона (8... 12,5 ГГц) для *уточнения характеристик цели,* точного ее сопровождения, отслеживания и распознавания.

Такая информационная подсистема позволяет обеспечить НПРО США:

- Глобальность действия – способность осуществлять уничтожение баллистических и аэродинамических стратегических средств до старта и стартующих из любой точки земного шара.
- Способность вести борьбу со средствами поражения на всех участках траектории их полета к цели.
- Глубокоэшелонированное построение системы ПРО, реализуемое применительно ко всем ее информационным, управляющим и ударным компонентам.
- Достижение в рамках системы ПРО такого системотехнического и конструктивного совершенства, которое обеспечивало бы решение задачи перехвата ударных средств противника прежде всего над его территорией на активном участке их траектории.

Рисунок 4

Структура системы систем оружия [18]



В этом случае система НПРО будет обеспечивать глобальное превосходство и максимальную защищенность США, одновременно вызывая нарушение достигнутого военно-стратегического паритета.

Детальное рассмотрение процессов функционирования данной *системы систем* показывает, что основным интегрирующим и системообразующим ее элементом является объединенная информационно-космическая подсистема.

Вместе с тем создание подобной системы оружия не позволяет в полной мере решить проблему защиты от применения оперативно-тактических ракет на территории европейских государств в условиях увеличения числа стран, владеющих баллистическими средствами вооруженной борьбы.

Как создать систему защиты от баллистических ракет, не вызывающую подозрений о намерениях у различных государств и не инициирующую гонку вооружений?

По мнению авторов, выявленный в ходе анализа перспективных систем ПРО информационно-интеграционный подход может быть использован для ускоренного формирования коллективной системы защиты от ракетной угрозы. В этом случае в создании наземного и орбитального информационных компонентов будут участвовать несколько государств, способных развернуть сегментированную наземно-орбитальную инфраструктуру, обеспечивающую эффективное функционирование коллективной системы ПРО [20] *(Рисунки 4 и 5).*

Рисунок 5

Наземно-орбитальный сегмент слежения за пусками ракет и их сопровождения на траектории полета к цели [21]

Рисунок 6

Наземно-орбитальный сегмент слежения за носителями баллистических ударных средств [22]

Представляется, что в таком случае системное пороговое значение числа КА ($N_{пор}$ $K_{пор}$) в информационных орбитальных группировках обеспечивается на основе численного суммирования КА отдельных сегментов, поэтому каждое отдельное государство не получает односторонних преимуществ в достижении скачкообразного повышения через космос эффективности национальных систем ПРО и национальных стратегических ИУСО.

Естественно, данное предложение носит концептуальный характер и для своей реализации потребует разработки развернутой программы по обеспечению его внедрения, что позволит создать условия по превращению космического пространства не в поле противоборства, а в арену сотрудничества.

Запретить нельзя одобрить

На сегодняшний день усилия международного сообщества направлены на международно-правовое запрещение испытаний и развертывания в космическом пространстве противоспутникового оружия. Использование подобного рода систем квалифицировалось бы с точки зрения международного права как вооруженное нападение на суверенное государство со всеми вытекающими из этого последствиями. В настоящий момент по действующим международно-правовым нормам государствам в космическом пространстве запрещено размещать отдельные виды оружия. Однако лишь после запрета противоспутникового оружия можно будет говорить об установлении в космическом пространстве международно-правового режима полной демилитаризации, исключающего из этого пространства в мирное время любые виды оружия.

В настоящее время остается нерешенной важнейшая проблема ограничения порогового значения для ИКС и сопряжения этих систем со средствами поражения.

Какие же международные организации потенциально могли бы и должны заняться столь существенной проблемой для глобальной безопасности? В первую очередь, необходимо отметить, что такой организацией, безусловно, является Организация Объединенных Наций, которая выступает в качестве центра согласования действий государств в мирном освоении космоса и выполняет возложенные на нее функции через свои главные и вспомогательные органы и смежные международные организации. Среди них следует особо выделить [23]:

- Комитет по использованию космического пространства в мирных целях (Комитет ООН по космосу);
- Управление по вопросам космического пространства (УКП);
- Институт ООН по исследованию проблем разоружения (ЮНИДИР);
- Международный союз электросвязи (МСЭ);

- Всемирная метрологическая организация (ВМО);
- Европейское космическое агентство (ЕКА);
- Европейская организация спутниковой связи (ЕВТЕЛСАТ);
- Международная организация подвижной спутниковой связи (ИНМАРСАТ);
- Комитет по исследованию космического пространства (КОСПАР);
- Ассоциация международного права;
- Международное общество фотограмметрии и дистанционного зондирования Земли (МОФДЗ).

Следует отметить, что в состав комитета ООН по космосу входят представители от 61 государства мира, что, безусловно, обеспечивает национальные интересы большей части государств мира. Для решения вышеуказанного спектра проблемных задач в системе регулирования военно-космической деятельности предлагается выделить новый важный элемент: *Комитет по ограничению и контролю за количественными характеристиками космических систем, способных быть включенными в контур боевого управления оружием, и недопущению использования в системах оружия космических аппаратов социально-экономического, научного и коммерческого назначения.* Указанный комитет в рамках развития существующей международно-договорной базы по использованию космического пространства был бы в состоянии рассмотреть вопрос по установлению такого международно-правового режима, который запрещал бы размещение в нем боевых средств и военного персонала. Данный режим предполагает:

- разработку международно-правовых норм по предотвращению гонки вооружений в космическом пространстве;
- разработку таких мер укрепления доверия, которые позволят исключить превращение космического пространства в театр военных действий и плацдарм для вооруженного нападения на другие государства.

Существующий сегодня международно-правовой режим, регламентирующий решение в космосе вопросов военно-космической деятельности (ВКД), не успевает за развитием ракетно-космической техники и технологий. Принимаемые политические меры также не в полной мере способны обеспечить эффективный контроль за развитием космических вооружений.

В этих условиях необходимо решить ряд задач международного сотрудничества, без которых немыслима всеобщая и устойчивая безопасность:

- укрепление и развитие существующих международно-правовых механизмов, обеспечивающих снижение уровня противостояния сторон и предупреждающих риск возрастания конфликтов в космическом пространстве;
- создание международно-правового режима по контролю над распространением технологий производства принципиально новых вооружений на основе сопряжения информационных систем с существующими ударными средствами.
- совершенствование международной системы обеспечения коллективной безопасности.

...И статистика

Существует еще одна серьезная проблема. Статистика показывает [24], что в годы Второй мировой войны для уничтожения такой типовой цели, как крупный железнодорожный мост через широкую реку, требовалось совершить 4,5 тыс. самолето-вылетов и сбросить около 9 тыс. авиабомб. В то же время за счет повышения точности поражения в войне во Вьетнаме подобная цель уничтожалась 190 авиабомбами, сброшенными 95 самолетами. В войне в Югославии эту же боевую задачу решали 1-3 высокоточные крылатые ракеты, запущенные с подводной лодки, находящейся в Средиземном море. Такое повышение точности возможно лишь при сопряжении ударных средств с космическими. Это сопряжение, безусловно, дает глобальное одностороннее преимущество стороне, которая обладает такими средствами поражения. Необходимо

установить международно-правовые ограничения на количественные характеристики ударных средств, сопряженных с космическими средствами. Конкретные данные по существующему арсеналу такого оружия и планам его производства указаны в *Таблице 1* [25].

Таблица 1

Арсенал высокоточного оружия ВВС и ВМС США и планы производства на 1 января 2007 г.[1]

Тип	Существующий арсенал	Планы производства	Планируемые затраты ($, млн)
Управляемые авиабомбы (УАБ)			
GBU-10	11 300		
GBU-12	32 600		
GBU-24/27	16 300		
GBU-28/GBU-37	125	225	**36**
*JDAM**			
*Navi**		25 496	641
*AF**		61 063	**1** 366
*JDAM-PIP**		5 000	
WCMD		40 000	508
SFW		3 413	**1** 150
Кассетные бомбы			
CBU-87 (Gator)	10 000		
CBU-89(CEM)	100 000		
CBU-97(SFW)	150	5 000	
Планирующие УАБ и управляемые ракеты			
CBU-15	2 800		
Maverrick	27 800		
Walleye	3 200		
AGM-142	130		
*JSOW(AGM-154)**			
*Baseline/BLU-108**		4 496	**1** 356
*Baseline/BLU-108(N) **		6 536	**1** 639
*Unitary**		3 194	**1** 692
AGM-130.	500	30	**26**
Крылатые ракеты средней дальности			
*SLAM**	770		
SLAM-ER/SLAM-ER PLUS*		423	256
*JASSM**		2 245	1278
Крылатые ракеты большой дальности			
*TLAM**	2 000		421
*Tact Tomahawk**	1253		**1** 278
CALCM+	90		

* Средства поражения, сопряженные с ИКС.

[1] На основе данных авторов.

Анализ существующего арсенала высокоточного оружия и перспектив его производства показывает, что США в достижении глобального превосходства основную ставку делают на создание средств поражения, сопряженных с ИКС, а это не что иное, как ИУСО.

Кодекс поведения

Принятие и выполнение соответствующего международно-правового акта в этой области при разработке соответствующего механизма контроля за его выполнением позволило бы не так остро ставить вопрос о глобальном превосходстве отдельных государств в космическом пространстве, что могло бы существенно снизить глобальную военную грозу. Такой контроль может достигаться на основе комплексной оценки общей численности функционирующих КА и их технических возможностей (с учетом наличия на орбитах КА как военного, так и двойного назначения).

Кроме того, в целях дальнейшего недопущения милитаризации космического пространства представляется целесообразным проведение следующих мероприятий:

- Заключение многосторонних международно-правовых соглашений, запрещающих испытание и развертывание в космическом пространстве любых видов оружия.
- Заключение международного соглашения об *иммунитете* искусственных спутников Земли.
- Определение и контроль пороговых значений количества КА в информационных ОГ, потенциально используемых в контуре боевого управления оружием.
- Создание международного космического инспектората и арбитражных органов космической инспекции.
- Разработка *кодекса поведения* в космическом пространстве (в том числе запрет опасных маневров, запрет маневров преследования, запрет опасных сближений, соблюдение минимальных дистанций между космическими объектами и т.д.).

Усилия ООН, других международных организаций в области международно-правового регулирования космической деятельности необходимо сосредоточить на создание такой нормативно-правовой базы, которая накладывала бы ограничения на количественные и качественные характеристики существующих и разрабатываемых космических систем военного и двойного назначения, способных быть включенными в контур боевого управления системами оружия.

Таким образом, можно сделать вывод о том, что распространение гонки вооружений на космос не может укрепить чью-либо безопасность. Создание систем оружия на основе широкого использования в их составе космических средств может привести к увеличению масштабов и числа участников военных конфликтов, так как космос является умножителем возможностей вооруженных сил государств мира. При этом государства, имеющие значительный космический потенциал, будут обладать серьезными стратегическими преимуществами. Для решения этих проблем необходимо плодотворное конструктивное сотрудничество всего мирового сообщества под эгидой ООН.

Источники и литература

1. Актуальные задачи развития ВС РФ. М.: МО, 2003. С. 19-21.
2. *Слипченко В.И.* Войны шестого поколения. М.: ВЕЧЕ, 2002. С.70, 121-123, 245-247, 303-303; *Юзвишин И.И.* Основы информациологии. М.: Международное издательство «Информациология», 2000. 517 с.
3. См. подробнее: *Гриняев С.Н.* «Сетевая война» по-американски. *Независимое Военное Обозрение.* 2002, № 5; *Слипченко В.И.* Бесконтактное истребление. *Независимое Военное Обозрение.*№ 21; *Монтгомери Мейгз.* Эпоха стратегической асимметричности. *Независимое Военное Обозрение.* 2002, № 37; *Золотарев В.А.* Сражение грядущего. *Независимое Военное Обозрение.* 2002, № 31. *Гриняев С.Н.* Война в четвертой сфере. *Независимое Военное Обозрение.* 2000, № 42; *Козлов Д.* Мир без мира, война без правил. *Независимое Военное Обозрение.* – 5 мая; *Баранов М., Тарасов С,*

Мухин Ю. Пушечное мясо для иракской войны. *Независимое Военное Обозрение.* – 2003, 12 декабря; *Кошкин А.* Обещание мирового масштаба. *Независимое Военное Обозрение.* 2003. – 5 декабря; *Новичков Н.* Ночное видение – ключ к успеху в современной войне. Независимое военное *Обозрение.* 2003,14 января.

4. *Слипченко В.И.* Там же.
5. *Васильев В., Лата В., Мальцев В.* Национальная система ПРО США: возможности и перспекти вы. *Ядерный Контроль.* 2002, № 2, том 8. С. 48-55.
6. *Мальцев В., Савыкин А.* От СОИ и ЕВРОСОИкширокомасшабнойсистемеПРОи ЕВРОПРО. Ра-*кетыи Космос.* 2002, № 3-4. С. 30-41.
7. National Missile Defence. What does it all mean? *CDI Issue Brief.* 2000, September, Washington. D.C. P. 10-16.
8. *Мальцев В., Савыкин А.* От СОИ и ЕВРОСОИ к широкомасшабной системе ПРО и ЕВРОПРО. *Ракеты и Космос.* 2002, № 3-4. С.30-41.
9. Киселев А.И., Медведев А.А., Меньшиков В.А. Космонавтика на рубеже тысячелетий. Итоги и перспективы. М.: Машиностроение. Машиностроение / Полет, 2001. С.27.
10. *Киселев А.И.* и др. Там же. С. 672.
11. *Мальцев В., Шавыкин А.* От СОИ и ЕВРОСОИ к широкомасштабной системе ПРО и ЕВРОПРО. *Ракеты и Космос.* 2002, № 3-4. С. 30-41.
12. Там же.
13. Там же.
14. Там же.
15. Там же.
16. Там же.
17. Там же.
18. Там же.
19. *Пудовкин О.Л., Андриянов Н.И., Ермак С.Н., Куликов С.В.* Космическая деятельность ООН и международных организаций. ЦИПК РВСН. 2001. С. 433.
20. *Слипченко В.И.* Там же.
21. *Мясников Е.* Высокоточное оружие и стратегический баланс. Центр по изучению проблем раз оружения, энергетики и экологии при МФТИ. 2000. С. 43.

Василий Лата
Владимир Мальцев

ХАКЕРЫ ОСТАНОВИЛИ СЕРДЦЕ[1]

Преступность в интернете дошла до физического устранения людей – прямо по проводам

Сбылся кошмар из голливудских триллеров. Убийцы лишили человека жизни дистанционно. Им не понадобились ни оружие, ни слежка. Вместо того чтобы нажать на курок, они просто нажали на кнопку клавиатуры.

Законодательства всех стран мира оказались не готовы к преступности в сфере высоких технологий. Эта незримая угроза, которую еще не почувствовали рядовые граждане, реально уже стоит на пороге нашего дома.

О том, с какими новыми преступлениями столкнулось одно из самых засекреченных управлений МВД, корреспонденту «Российской газеты» рассказал полковник управления «К» Анатолий Платонов.

Когда компьютер страшнее пистолета

– Интернет лишь недавно вошел в наш обиход, по юридическим меркам – вчера. И сразу в печати и по телевидению стали появляться жуткие рассказы и фильмы о хакерах, которые ловко обводят вокруг пальца правоохранительные органы.

– Я не люблю слово «хакер» в применении к компьютерным преступникам. Если вы посмотрите в словарь, то ни одно из значений этого слова не носит криминальный характер. Если говорить о преступном мире в интернете, то более применимо словосочетание «компьютерные взломщики». Хотя и оно не отражает всего спектра того, что происходит в сети.

– Что вы имеете в виду?

– Сейчас в сети зарегистрированы практически все виды преступлений, кроме изнасилования. Даже убийства через интернет уже случались. Известный случай из практики США. Там пострадавший от покушения не погиб от пуль, а лишь был тяжело ранен. Попав под программу защиты свидетелей, человек был помещен полицией в охраняемую палату, но преступники через интернет вошли в сети клиники, где он лежал, и, что называется, «достали» его с помощью хай-тек. Изменив программу прибора стимуляции сердца, злоумышленники добили жертву.

– Это воспринимается почти как фантастика и, думается, что подобные случаи скорее исключение из правил. По крайней мере, пока.

– Ничего подобного. В интернете уже сейчас идет настоящая невидимая война.

– Насколько наши правоохранительные органы к ней готовы?

– Готовы. Если говорить о квалификации кадров, если говорить о показателях. Скажем, такой известный вид преступлений, как организация незаконных переговорных пунктов, сотрудникам управления «К» почти удалось победить. Если вы помните, еще совсем недавно телекоммуникационные компании России несли огромные убытки из-за того, что преступники, в основном это были представители вьетнамской диаспоры, использовали вредоносные программы, чтобы созваниваться с земляками и родственниками по всему миру. После ряда арестов хорошо организованные этнические диаспоры приняли решения отказаться от совершения такого вида преступлений. Появились новые виды криминала, так называемые роуминговые, связанные уже с сотовой связью.

---

[1] «Российская газета», 8 февраля 2005г. http://www.rg.ru/2005/02/08/e-prestupnost.html

Виртуальный секс с реальными сроками

– Где же выход? И значит ли это, что компьютерные преступники, бывает, остаются безнаказанными?

– Как правило, негодяи получают свое по полной. Просто специфика раскрытия преступлений в сфере хай-тек такова, что законодательство всегда отстает. Это закономерно. Приходится применять к ним, так сказать, классические, проверенные что ли статьи УК РФ. Например, статьи за мошенничество или вымогательство, ведь так или иначе почти любое преступление связано либо с обманом, либо с жаждой денег.

Скорость изменения преступлений в сфере хай-тек такова, что законодательная база немного опаздывает. Эта проблема не только российская, но и общемировая.

Нашими сотрудниками в интернете был найден сайт, где за деньги предлагались видеоматериалы порнографического содержания с участием несовершеннолетних. В процессе оперативной игры был налажен контакт с продавцом. Им оказался лаборант одной из пермских школ по фамилии Пиньевский (фамилия несколько изменена). Он легко пошел на то, чтобы по заказу оперативников снять фильм с девочкой шести лет. Впоследствии выяснилось, что «моделей» для съемок 27-летнему лаборанту предоставлял несовершеннолетний сутенер. На видеопленке зафиксировано, как Пиньевский встречался с ним. Финальная часть операции проходила в одном из классов школы, где работал лаборант и где также работала его мать. По легенде оперативники под видом покупателей должны были присутствовать при съемках порнофильма с участием Пиньевского и семилетней девчушки. От прокурора было получено указание, не дать извращенцу шанса надругаться над ребенком или его испугать. В дальнейшем при обыске дома у арестованного были найдены многочисленные видеофильмы с участием его и малолетних. Ему было предъявлено обвинение по нескольким статьям, но суд, который состоялся в прошлом году, посчитал вину подсудимого... недоказанной. Основания следующие – это якобы оперативники спровоцировали его на совершение развратных действий.

Оправдательные приговоры таким, как Пиньевский, – не правило, а, скорее, исключение. За последнее время региональные подразделения управления «К» выявили и пресекли деятельность педофилов в Башкирии, в Туле, где действовал интернет-сайт «Детский сад», в Тамбове, где видеодиски продавал студент летно-технического училища, его, кстати, так и взяли в форме курсанта, в Стерлитамаке, где видеопродукцией торговал 33-летний программист.

– Но, как я понимаю, вы боретесь не только с педофилами?

– Нет, конечно. Если говорить о хорошо знакомых нам видах преступления в сети, то это прежде всего борьба с создателями вредоносных компьютерных программ.

Например, оперативниками управления в Ленинградской области был пойман один из инженеров, который разработал программу, с помощью которой практически все торговые точки России могли уходить от налогов. Хитроумная в прямом смысле слова новация криминального изобретателя могла стирать или изменять фискальную память в контрольно-кассовых аппаратах.

С поставленным на промышленную основу изготовлением измененных контрольно-кассовых аппаратов оперативники столкнулись весной прошлого года. За продажу таких кассовых аппаратов были привлечены к ответственности фирмы в Москве и Калужской области. В Москве на складе были обнаружены десятки тысяч складированных и готовых к продаже машин.

Может, это и не броское преступление по сравнению с убийством по проводам, но, по данным экспертов из министерства по налогам и сборам, из-за таких преступлений казна несет убытки в размере 200 миллиардов рублей в год.

Угроза от бен Ладена – из Барнаула

– Но в любом случае – это не преступление из разряда давно всем знакомых «убил, зарезал, задушил».

– Да, управление «К» как раз в основном и сталкивается с нетрадиционными видами преступлений, некоторые из которых бывают весьма забавными. Например, 20 июня 2004г. был осужден первый в России спамер. Спам – это компьютерная рассылка, которую получатель не заказывал и получать не хочет. Иначе говоря, это компьютерный мусор, который засоряет интернет и электронные ящики компьютерных пользователей.

Так вот, некий гражданин Д.Андросов из уральского города Челябинска написал программу, которая производила автоматическую отсылку SMS-сообщений на сотовые телефоны. Чтобы скомпрометировать одну сотовую компанию, Андросов запустил программу с одного из серверов Санкт-Петербурга. В результате более 16 тысяч человек получили на сотовые телефоны послания нецензурного содержания. Представляете, папа купил своему восьмилетнему сыну на день рождения мобильник. Тот его включил, а телефон матерится и ребенка на три буквы посылает.

На суде Андросов получил год условно и штраф в размере трех тысяч рублей.

– Не слишком сурово.

– Понимаете, главное прецедент. Ведь это весьма редкое для России дело. Спамеров ненавидят во всем цивилизованном мире, но осудить не могут. В 2004г. в США впервые был осужден спамер, он получил семь лет лишения свободы. Челябинское дело еще раз показало, что российские правоохранительные органы могут успешно раскрывать преступления, связанные с распространением спама, но не всегда хватает правового базиса.

– Какие еще громкие дела расследовало управление «К»?

– Очень интересное дело было в прошлом году по обнаружению авторов «атаки на Америку».

Все началось с того, что на сайте ЦРУ в Лэнгли появилось предупреждение о предстоящих взрывах в нью-йоркском метро. И хотя сообщение сопровождалось словами «Аллах акбар» и было подписано бен Ладеном, американские специалисты установили, что сообщение пришло из российского сегмента сети интернет. Но меньше тревоги у американцев от этого не стало. Они немедленно остановили метро и начали поиски бомбы. Одновременно по каналам международного взаимодействия в МВД России обратились сотрудники ФБР.

Наши специалисты установили, что послание было отправлено из Барнаула. Был вычислен не только институт, но аудитория и компьютер, с которого отправилось письмо. И все это, заметьте, в течение одних суток. ФБР обратилось за помощью к специалистам управления «К». Для ФБР важна была скорость. В два часа ночи в Барнауле была создана оперативно-поисковая группа, которая к утру и нашла злоумышленника. А как иначе, ведь метро в Нью-Йорке стоит, пассажиров эвакуировали, сыграли оранжевую тревогу, все сыщики ищут бомбу, а серьезность угрозы оценить невозможно.

Это лишь потом выяснилось, что никакой бомбы не было, а один из барнаульских студентов, которого арестовали и затем осудили, просто решил «пошалить».

Вирусная атака на миллионеров

– С какими самыми экзотическими видами компьютерных преступлений вам пришлось сталкиваться?

– Думаю, к таким преступлениям вполне можно отнести так называемые Д-ДОС-атаки. Это настолько специфичный в мировой практике вид преступлений, что, описывая его, надо

еще постараться подобрать слова. Хотя эти преступления можно в равной степени причислить и к одним из самых опасных и громких.

До прошлого года сотрудникам нашего управления доводилось сталкиваться лишь с ДОС-атаками, когда вирусы и различные вредоносные программы атакуют чужие серверы и затрудняют работу предприятий и компаний. Впервые с ДОС-атаками мы столкнулись в прошлом году в Ижевске, когда были атакованы филиалы крупных российских банков. Сотрудники управления «К» тогда раскрыли это преступление, которое с натяжкой можно было назвать атакой вредоносными программами.

В прошлом же году в течение одиннадцати месяцев девять брокерских контор в Англии и Уэльсе подвергались нападению с помощью Д-ДОС-атак, которые оказались куда опаснее ДОС-атак. Некоторые следы привели в Россию. Для нас это так же, как и для англичан, был совершенно новый вид преступления. Но, как показала практика, наши специалисты оказались ничуть не хуже сотрудников Скотленд-Ярда, которые прибыли в Москву для взаимодействия в раскрытии этого преступления. Была создана общая оперативно-следственная группа и общее уголовное дело.

Расследование показало, что в сети действует своеобразный компьютерный интернационал в худшем смысле этого слова. Они даже не знали друг друга в лицо. Пароль для сближения – виртуозное владение программированием. Это люди, которые практически живут в сети и снюхиваются по той известной поговорке, как рыбак рыбака.

Так сложилась и эта международная преступная группа, которая запускала в компьютерные сети британских банков и контор некие «боты», это с английского – лодки.

Так вот, преступники запускали с различных компьютеров в разных странах эти невидимые кораблики в море Интернета, которые не обнаруживала ни одна из антивирусных программ. До поры до времени эти «боты» никак не проявляли себя в чужих сетях. Но стоило, например, подойти времени делать ставки на тотализаторе, как сервер букмекерской конторы мог быть парализован, в результате чего предприниматели на бегах несли огромные убытки.

Досье «РГ»

Всего управлением «К» раскрыто 94% преступлений в сфере распространения порнографии, зарегистрированных ГИЦ МВД за 2003г. Тем не менее, в 2004г. приняты дополнения в УК РФ, по которым предусмотрена уголовная ответственность за такие преступления до восьми лет лишения свободы. Они отнесены к разделу тяжких. Просматривается такая тенденция – на фоне увеличения преступлений, связанных с распространением порнографии, количество преступлений с детской порнографией значительно снизилось.

Тимофей Борисов

СПРОС НА РЕШЕНИЯ ЖДЕТ СВОЕГО ПРЕДЛОЖЕНИЯ

Стремление изменить существующее состояние к лучшему – одна из самых важных, если не важнейшая черта человеческой природы.

Но чтобы двигаться в желаемом направлении, необходимо иметь представление о хотя бы некоторых параметрах этого лучшего состояния.

В экономическом аспекте критерием лучшего до недавнего времени являлся показатель валового внутреннего продукта (ВВП) на душу населения.

С этим показателем было связано понятие «развитие страны», на которое должен был равняться весь мир, и дающее почву для многочисленных сравнений: «у нас так, а у них вот так».

Правомерность использования показателя ВВП на душу населения для линейного ранжирования стран была поставлена под сомнение, прежде всего, в самих США, сторонниками мощного научного направления – эволюционной теории.

Многими экспертами как на Западе, так и в СНГ высказывалось мнение (сторонником которого является и автор статьи), что здесь имеет место политика двойных стандартов: в практике внутринациональной жизни США весомо учитывают выводы эволюционной теории, в то время как остальному миру навязываются, в основном, догмы монетаризма.

Приведем две основные причины некорректности использования показателя ВВП на душу населения.

В состав ВВП по существующей методологии входит добавленная стоимость всех предприятий, имеющих прибыль. По оценкам эволюционистов, львиную долю этой стоимости составляют услуги юридического сектора, являющегося важнейшей частью трансакционного сектора.

На современном этапе проблемой N1 развития любой страны выступает стремление трансакционного сектора активно расширять свою сферу за счет намеренного усложнения законодательного поля и усиления бюрократизации страны.

К сожалению, все это уже получило свое достаточно яркое отображение и в Армении, т.е. заимствование внешнего опыта идет, почему-то, прежде всего по негативным аспектам. Достаточно обратиться к структуре абитуриентов, тяготеющих, в основном, к юриспруденции и экономике. Значительная часть из них осознанно стремиться не в сферу бизнеса, а на стык государства и бизнеса для получения доходов от паразитной нагрузки на последний.

Имеет смысл также проанализировать ситуацию с законодательным полем налогообложения бизнеса: усложняется оно или упрощается и насколько стремится соответствовать реалиям Армении? Желательно периодически освещать в прессе оценку этого процесса со стороны самих предпринимателей. В целом это сводится к вопросу: в какой степени институциональное развитие ориентировано на раскрытие потенциала личности, а в какой – на создание комфортной среды для определенных групп?

Вторая причина некорректного использования показателя ВВП в том, что один и тот же объем ВВП может быть получен как за счет экспорта сырья, полуфабрикатов и т.д., так и за счет высоких технологий.

Наконец-то это поняли и у нас, и на самом высоком уровне – президентском, отметили, что высокие темпы ВВП за счет жилищного строительства – не повод для эйфории.

Вместе с тем опыт «развитых стран», без сомнения, несет в себе определенную позитивную информацию.

В этой связи хотелось бы остановиться на макропоказателях, характеризующих уровень взаимосвязи личности и экономики и уровня эффективности отраслевой структуры и государственного воздействия.

1. Первый из них связан с показателем доли оплаты труда в ценах реализации. На макроуровне этот показатель коррелирует с отношением оплаты труда к валовому выпуску. К сожалению, в *IFS* отсутствуют данные о валовом выпуске по зарубежным странам и пришлось не очень корректно заменить его отношением оплаты труда к ВВП. Для Германии, Исландии, Франции, Турции этот показатель в 2004г. составил соответственно 50%, 52%, 51% и 25%.

Высокий уровень этого показателя свидетельствует о том, что оплата труда (а косвенно – и личность) выступает ценообразующим фактором. Его значение для Армении – 40%, взято, по-видимому, из расчета средней зарплаты 65000 драм на 1.200.000 занятых, мягко говоря, не вызывает доверие. Есть все основания считать, что его уровень как минимум не лучше турецкого.

Понимание социально-экономической значимости этого показателя восходит ко временам Великой депрессии 1929г. в.США, когда из-за низкого уровня платежеспособного спроса населения емкость внутреннего рынка упала ниже критической отметки.

Администрация Ф.Рузвельта сумела довести до общественного сознания, что низкий уровень оплаты труда, вызванный эгоизмом экономической верхушки, самоубийственен для экономики в целом и в конечном счете – для самих предпринимателей.

Экономический аспект рассматриваемого показателя тесно переплетается с социальным: низкий уровень оплаты труда порождает развращенность экономических верхов, незаинтересованность в качественном труде у работающих, и в конечном счете создает напряженность в обществе и пессимизм в оценке будущего.

У рассматриваемого макропоказателя есть и другой, не менее важный аспект, связанный с уровнем и структурой внутреннего спроса.

Сегодня можно считать общеизвестным тот факт, что внутреннее экономическое пространство находится под контролем относительно небольшого круга лиц, называемых олигархами.

Этот фактор плюс специфика современного национального менталитета – стремление минимально зависеть от своих, создают выталкивающую среду под влиянием которой создаются предприятия по договоренности с внешними деловыми кругами, обусловленными благоприятной политико-экономической конъюктурой.

В результате определенную часть экономики можно представить, как отдельные технологические нитки, которые объединяет только общая инфраструктура: энергетика, транспорт, связь.

Эти предприятия чрезвычайно чувствительны к обусловившей их создание внешней конъюктуре.

Однако именно нестабильность общемировой среды является сегодня по практически единодушному мнению экспертов ее важнейшим индикатором, характеристикой.

Это значит, что с высокой долей вероятности та или иная часть этих предприятий уже оказалась и будет оказываться в кризисной ситуации.

Решением здесь является не требование компенсировать внешние риски курсом национальной валюты, а продуманная государственная политика, направленная на создание предприятий, которые с одной стороны в достаточной мере связаны между собой, а с другой – идут в авангарде мирового спроса или формируют его (инновационная экономика).

В этом контексте разговоры о ставке на дешевый труд – рецидив феодального мышления, перекрывающий пути к радикальным решениям.

2. Сравнительный межстрановый анализ макропоказателя отношения доходной части бюджета к ВВП (по данным 1998г). Германия – 31%, Франция – 40%, Армения – 16.7% (2005г)

позволяет определиться со следующими весьма важными аспектами экономической и общественной систем.

Первый аспект связан с уровнем стратегирования в обществе. Высокий уровень этого показателя означает, что значительная часть ВВП перераспределяется государством, исходя из определенных долговременных стратегических целей. В частности, это также означает, что на современном этапе создание новых перспективных направлений в экономике требует наличия централизованного органа, ответственного за стратегию развития, и эту миссию государство берет на себя.

Думать, что формирование этих направлений произойдет само собой, по законам рынка – и наивно, и опасно в современном жестко конкурирующем мире.

Второй аспект носит более опосредованный, но не менее важный характер.

Экономика любой страны функционирует в среде воздействия государства, оказывающего где стимулирующее, а где – сдерживающее влияние.

Эффективность экономики в решающей степени зависит от того, насколько структура этого воздействия соответствует текущим и перспективным общемировым тенденциям (на данном этапе – создание инновационной экономики) с одной стороны, и специфике человеческих и природных ресурсов – с другой.

Чем более адекватна структура государственного воздействия задачам развития, тем большее налоговое бремя может выдержать экономика.

Необходимым условием такого воздействия принято считать размежевание государства и бизнеса.

В Армении в результате сращивания государственного аппарата и бизнеса сложилась определенная патронажная отраслевая структура.

Если предположить, что государство внезапно стало нейтральным по отношению к бизнесу и решило довести этот показатель до уровня развитых стран, то существующая отраслевая структура просто не выдержит этой нагрузки из-за своей недостаточной эффективности, которая, в основном, базируется на ценовом беспределе в условиях монополизированности рынков и государственного патронажа.

Все вышесказанное оказывает свое влияние и на денежную систему. Выполняемые деньгами функции можно сформулировать как платежно-расчетную, сбережений и меры. Последняя функция через соотношение цен выражает соотношение полезностей (потребительской стоимости) и затратами (стоимостью) для различных товаров и услуг по отношению друг к другу.

Теоретический спор, что первичнее – субъективная полезность или объективная стоимость, суммировал в свое время известнейший экономист А.Маршалл, сравнив их с двумя частями ножниц – одно предполагает другое.

Полное расстройство денежной системы означает, что под угрозой все три функции. Такое может произойти, например, в условиях гиперинфляции.

Возможен, однако, вариант, когда под угрозу попадает вначале третья функция – меры, которая наиболее чувствительна к экономической структуре. Такая ситуация возникает, например, в условиях монополизированности рынков и неадекватного государственного патронажа, как это имеет место в Армении. В этом случае соотношение цен слабо связано и с полезностью, и с затратами. Если такая ситуация продлиться достаточно долго, то под угрозой неизбежно окажутся и остальные функции.

Это в свою очередь снижает ресурс денежно-кредитной политики.

Вообще, в условиях искривленной экономики упование только на монетарные рычаги опасно, особенно в случае их форсированного использования.

Денежно-кредитная политика – действительно мощный рычаг, но не настолько, чтобы исправить структуру сращенной государственно-экономической системы.

Отдельно хотелось бы остановиться на следующем психологическом феномене.

Оставляя в стороне фактор компетентности авторов многочисленных публикаций с рецептами спасения отечества, хочется задать вопрос: кому они адресованы?

Создается ощущение, что неявно ставится задача наполнения некоего информационного поля попутно с выпусканием «пара»: авторы как бы выполняют свой долг перед Родиной и, испытывая зуд деятельности, обращаются к рычагам, лежащим на поверхности – денежно-кредитной политике.

Вместе с тем даже безадресное (имеется в виду умалчивание того, кто это может и заинтересован делать), но объективное, содержательное наполнение информационного поля имеет смысл, т.к. создает определенный общественный спрос, который рано или поздно найдет свое предложение.

Это предложение, так или иначе, будет связано с созданием организационного потенциала, ориентированного на решение национальных задач. С этой целью будет необходимо связать в единое целое сверху вниз отдельные фрагменты тех уже действующих организационных ресурсов, которые готовы взять на себя миссию решения стратегических национальных задач.

Игорь Багирян