ՀԱՄԱՁԱՅՆԱԳԻՐ

Հայաստանի Հանրապետության կառավարության և Ռուսաստանի Դաշնության կառավարության միջև տեղեկատվական անվտանգության ապահովման բնագավառում համագործակցության մասին

Հայաստանի Հանրապետության կառավարությունը և Ռուսաստանի Դաշնության կառավարությունը, այսուհետ՝ Կողմեր,

ընդգծելով միջազգային տեղեկատվական անվտանգության ապահովման հարցում էական ազդեցություն ունեցող՝ տեղեկատվական-հաղորդակցական տեխնոլոգիաների զարգացման և ներդրման զգալի առաջընթացը,

ղեկավարվելով «Հայաստանի Հանրապետության և Ռուսաստանի Դաշնության միջև բարեկամության, համագործակցության և փոխադարձ օգնության մասին» 1997թ. օգոստոսի 29-ի պայմանագրով,

ընդգծելով տեղեկատվական-հաղորդակցական տեխնոլոգիաների մեծ նշանակությունը սոցիալ-տնտեսական զարգացման համար՝ ի շահ մարդկության, ինչպես նաև միջազգային խաղաղության, անվտանգության և կայունության պահպանության համար,

մտահոգություն հայտնելով միջազգային խաղաղության, անվտանգության և կայունության ապահովման խնդիրների հետ անհամատեղելի նպատակներով, պետությունների ինքնիշխանությունն ու անվտանգությունը խաթարելու և նրանց ներքին գործերին միջամտելու, ներքաղաքական և սոցիալ-տնտեսական իրավիճակի ապակայունացման, ազգամիջյան և միջկրոնական թշնամանքի հրահրման համար տեղեկատվական-հեռահաղորդակցական տեխնոլոգիաների օգտագործման հնարավորությունների հետ կապված սպառնալիքների առնչությամբ,

կարևորելով միջազգային տեղեկատվական անվտանգությունը՝ որպես միջազգային անվտանգության համակարգի առանցքային տարրերից մեկը,

աջակցելով տեղեկատվական տարածքում Միավորված ազգերի կազմակերպության հովանու ներքո պետությունների պատասխանատու վարքագծի միջազգային կանոնների, նորմերի և սկզբունքների մշակմանն ու ընդունմանը՝ բոլոր երկրների համար հավասար անվտանգության ապահովմանը նպաստելու համար,

հաստատելով «Ինտերնետ» տեղեկատվական-հեռահաղորդակցական ցանցի հետ կապված հարցերի վերաբերյալ պետական քաղաքականություն սահմանելու և վարելու պետությունների ինքնիշխան իրավունքը, ներառյալ դրա անվտանգ և կայուն գործունեության ապահովումը,

համոզված լինելով, որ տեղեկատվական-հաղորդակցական տեխնոլոգիաների օգտագործման բնագավառում Կողմերի փոխգործակցության հետագա խորացումն ու զարգացումը համապատասխանում է իրենց շահերին,

կարևորելով տեղեկատվական-հաղորդակցական տեխնոլոգիաների օգտագործման ոլորտում անվտանգության ապահովման և մարդու իրավունքների պաշտպանության միջև հավասարակշռությունը՝ Կողմերի պետությունների ազգային օրենսդրություններին, ինչպես նաև միջազգային պարտավորություններին համապատասխան,

ձգտելով կանխել միջազգային տեղեկատվական անվտանգության սպառնալիքները և ապահովել Կողմերի պետությունների ազգային շահերը տեղեկատվական բնագավառում,

ցանկանալով ստեղծել տեղեկատվական անվտանգության բնագավառում Կողմերի՝ երրորդ կողմի շահերին չուղղված համագործակցության իրավական և կազմակերպչական հիմքեր,

համաձայնեցին հետևյալի մասին.

Հոդված 1

Տեղեկատվական անվտանգության ապահովման բնագավառում առկա հիմնական սպառնալիքները

Սույն Համաձայնագրին համապատասխան համագործակցություն իրականացնելիս Կողմերը ելնում են նրանից, որ տեղեկատվական անվտանգության ապահովման բնագավառում հիմնական սպառնալիքներն են.

1) տեղեկատվական-հաղորդակցական տեխնոլոգիաների օգտագործումը՝ Կողմերի պետությունների ինքնիշխանության, անվտանգության և տարածքային ամբողջականության խախտմանն ուղղված գործողությունների իրականացման համար,

2) տեղեկատվական-հաղորդակցական տեխնոլոգիաների օգտագործումը՝ կրիտիկական տեղեկատվական ենթակառուցվածքի օբյեկտների վրա ապակառուցողական ներգործություն ունենալու համար,

3) տեղեկատվական-հաղորդակցական տեխնոլոգիաների օգտագործումը՝ ահաբեկչական նպատակներով, այդ թվում՝ ահաբեկչության քարոզչության և ահաբեկչական գործունեության մեջ ներգրավելու համար,

4) տեղեկատվական-հաղորդակցական տեխնոլոգիաների օգտագործումը՝ համակարգչային տեղեկատվության ոլորտում հանցագործություններ կատարելու համար, այդ թվում՝ Կողմերի տեղեկատվական ռեսուրսների, համակարգչային տեղեկատվության ոչ օրինաչափ հասանելիության և օգտագործման, համակարգչային վնասակար ծրագրերի ստեղծման, օգտագործման և տարածման, համակարգչային տեղեկատվության պահպանման, մշակման կամ փոխանցման միջոցների ու տեղեկատվական-հեռահաղորդակցական ցանցերի շահագործման կանոնների խախտման հետ կապված, ինչպես նաև այլ հանցավոր նպատակներով,

5) տեղեկատվական-հաղորդակցական տեխնոլոգիաների օգտագործումը՝ Կողմերի պետությունների ներքին գործերին միջամտելու, հասարակական կարգի խախտման, ազգամիջյան, միջռասայական և միջկրոնական թշնամանք հրահրելու, ատելություն և խտրականություն ծնող, բռնության ու անկայունության դրդող ռասիստական և այլատյաց գաղափարներ ու տեսություններ քարոզելու, ինչպես նաև ներքաղաքական և սոցիալ-տնտեսական իրավիճակի ապակայունացման, պետության կառավարումը խաթարելու համար,

6) տեղեկատվական-հաղորդակցական տեխնոլոգիաների օգտագործումը՝ Կողմերի պետությունների հասարակական-քաղաքական և սոցիալ-տնտեսական համակարգերին, հոգևոր, բարոյական և մշակութային միջավայրերին վնասող տեղեկատվության տարածման համար:

Հոդված 2

Համագործակցության ընդհանուր սկզբունքները

1. Կողմերը սույն Համաձայնագրի շրջանակներում տեղեկատվական անվտանգության ապահովման ոլորտում համագործակցությունն իրականացնում են այնպես, որ նշված համագործակցությունը նպաստի սոցիալական և տնտեսական զարգացմանը, համատեղելի լինի միջազգային խաղաղության, անվտանգության ու կայունության պահպանման խնդիրների հետ և համապատասխանի միջազգային իրավունքի համընդհանուր ճանաչում ունեցող սկզբունքներին ու նորմերին, ինչպես նաև երկկողմ համագործակցության և Կողմերի պետությունների տեղեկատվական ռեսուրսներին չմիջամտելու սկզբունքներին:

2. Կողմերի գործունեությունը սույն Համաձայնագրի շրջանակներում իրականացվում է Կողմերի պետությունների ազգային օրենսդրություններին համապատասխան:

3. Յուրաքանչյուր Կողմ ունի իր պետության տեղեկատվական ռեսուրսները ոչ օրինաչափ օգտագործումից և չարտոնված միջամտությունից, այդ թվում՝ դրանց վրա համակարգչային հարձակումներից պաշտպանելու հավասար իրավունքներ: Յուրաքանչյուր Կողմ չի իրականացնում մյուս Կողմի նկատմամբ նման գործողություններ և աջակցություն է ցուցաբերում մյուս Կողմին նշված իրավունքների իրականացման գործում:

4. Կողմերը ջանքեր են գործադրում, որ Կողմերի պետությունների տեղեկատվական ենթակառուցվածքը և ռեսուրսները որևէ երրորդ կողմ չօգտագործի Կողմերի պետություններին վնաս հասցնելու համար:

Հոդված 3

Համագործակցության հիմնական ուղղությունները

1. Սույն Համաձայնագրի շրջանակներում Կողմերի պետությունների իրավասու մարմինները, որոնք սահմանվում են սույն Համաձայնագրի 5-րդ հոդվածին համապատասխան, տեղեկատվական անվտանգության ապահովման բնագավառում համագործակցություն են իրականացնում հետևյալ հիմնական ուղղություններով.

1) սույն Համաձայնագրի 1-ին հոդվածում նշված տեղեկատվական անվտանգության ապահովման ոլորտի սպառնալիքներին հակազդման համակարգում,

2) իրավապահ ոլորտում տեղեկատվության փոխանակում՝ ահաբեկչական և այլ հանցավոր նպատակներով տեղեկատվական-հաղորդակցական տեխնոլոգիաների օգտագործման հետ կապված

իրավախախտումները բացահայտելու, կանխարգելելու, կանխելու և քննելու նպատակով,

3) տեղեկատվական անվտանգության ապահովմանը նպաստող վստահության անհրաժեշտ միջոցառումների համաձայնեցում և իրականացում,

4) Կողմերի պետությունների իրավասու մարմինների միջև տեղեկատվական անվտանգության ապահովման հարցերով տեղեկատվության փոխանակում, ներառյալ համակարգչային միջադեպերի արձագանքման ոլորտում համագործակցությունը,

5) տեղեկատվական անվտանգության ապահովման հարցերի վերաբերյալ Կողմերի պետությունների օրենսդրության մասով տեղեկատվության փոխանակում,

6) տեղեկատվական անվտանգության ապահովման բնագավառում Կողմերի պետությունների համագործակցության երկկողմ նորմատիվ իրավական բազայի և գործնական մեխանիզմների կատարելագործում,

7) ազգային և միջազգային տեղեկատվական անվտանգության ապահովման նպատակով մասնակցություն միջազգային իրավունքի մշակմանն ու առաջմղմանը,

8) միջազգային կազմակերպությունների և համաժողովների շրջանակներում (ներառյալ Միավորված ազգերի կազմակերպությունը, Էլեկտրակապի միջազգային միությունը, Եվրոպայում անվտանգության և համագործակցության կազմակերպությունը, Հավաքական անվտանգության պայմանագրի կազմակերպությունը, Անկախ Պետությունների Համագործակցությունը և այլն) միջազգային տեղեկատվական անվտանգության ապահովման խնդիրների լուծման գործում Կողմերի պետությունների փոխգործակցության և գործունեության համակարգում,

9) տեղեկատվական անվտանգության ոլորտում Կողմերի պետությունների լիազորված ներկայացուցիչների և փորձագետների

աշխատանքային հանդիպումների, գիտաժողովների, սեմինարների և այլ համաժողովների անցկացում,

10) փոխգործակցություն տեղեկատվական անվտանգության ոլորտում կադրերի պատրաստման, ստաժավորումների, մասնագետների փոխանակման ոլոտում,

11) տեղեկատվական անվտանգության բնագավառում օրենսդրության կատարելագործման հարցերով փորձի փոխանակում,

12) աջակցություն տեղեկատվական անվտանգության ապահովման հարցերով գիտահետազոտական գործունեության իրականացմանը:

2. Կողմերը կամ Կողմերի պետությունների իրավասու մարմինները գրավոր պայմանավորվածությամբ կարող են որոշել համագործակցության այլ ուղղություններ:

Հոդված 4

Համակարգող մարմինները

Սույն Համաձայնագրի դրույթների արդյունավետ իրականացմանը նպաստելու և Հայաստանի Հանրապետության ու Ռուսաստանի Դաշնության միջև անմիջական փոխգործակցություն հաստատելու նպատակով սույն Համաձայնագրի շրջանակներում որպես համակարգող սահմանվել են հետևյալ մարմինները.

Հայաստանի Հանրապետության կողմից՝ Հայաստանի Հանրապետության անվտանգության խորհրդի գրասենյակը,

Ռուսաստանի Դաշնության կողմից՝ Ռուսաստանի Դաշնության անվտանգության խորհրդի գրասենյակը:

Անհրաժեշտության դեպքում Կողմերը կարող են փոխել համակարգող մարմինը՝ այդ փոփոխությունների մասին դիվանագիտական ուղիներով մյուս Կողմին անհապաղ գրավոր ծանուցելով:

Հոդված 5

Համագործակցության ձևերն ու մեխանիզմները

1. Սույն Համաձայնագրով նախատեսված համագործակցության կոնկրետ ուղղություններով գործնական փոխգործակցությունը Կողմերը կարող են իրականացնել սույն Համաձայնագրի իրագործման համար պատասխանատու՝ Կողմերի պետությունների իրավասու մարմինների գծով: Սույն Համաձայնագրի ուժի մեջ մտնելուց հետո՝ 60 օրվա ընթացքում, Կողմերը դիվանագիտական ուղիներով փոխանակում են սույն Համաձայնագրի իրագործման համար պատասխանատու՝ Կողմերի պետությունների իրավասու մարմինների մասին տվյալները:

2. Կոնկրետ ուղղություններով համագործակցության իրավական և կազմակերպչական հիմքերի ստեղծման նպատակով Կողմերի պետությունների իրավասու մարմինները կարող են կնքել համապատասխան պայմանագրեր:

3. Սույն Համաձայնագրի իրագործման ընթացքի ուսումնասիրության, տեղեկատվության փոխանակման, տեղեկատվական անվտանգության սպառնալիքների վերլուծության և համատեղ գնահատման, այդ սպառնալիքներին արձագանքելու համատեղ միջոցառումների սահմանման, համաձայնեցման և համակարգման նպատակով Կողմերը կանոնավոր կերպով անցկացնում են Կողմերի պետությունների իրավասու մարմինների ներկայացուցիչների մասնակցությամբ միջգերատեսչական խորհրդակցություններ, ինչպես նաև Կողմերի պետությունների իրավասու մարմինների խորհրդակցություններ:

Միջգերատեսչական խորհրդակցություններն անցկացվում են Կողմերի համաձայնեցմամբ, տարին առնվազն մեկ անգամ՝ հաջորդաբար Հայաստանի Հանրապետությունում և Ռուսաստանի Դաշնությունում, իսկ իրավասու մարմինների խորհրդակցությունները՝ տվյալ մարմինների համաձայնեցմամբ:

Կողմերից յուրաքանչյուրը կարող է նախաձեռնել լրացուցիչ խորհրդակցությունների անցկացում՝ առաջարկելով դրանց անցկացման ժամանակն ու վայրը, ինչպես նաև օրակարգը:

Հոդված 6

Տեղեկատվության պաշտպանությունը

Կողմերն ապահովում են սույն Համաձայնագրի շրջանակներում համագործակցության ընթացքում փոխանցվող կամ ստեղծվող տեղեկատվության պատշաճ պաշտպանությունը, որի հասանելիությունը սահմանափակված է Կողմերի պետությունների ազգային օրենսդրությանը համապատասխան:

Այդպիսի տեղեկատվության պաշտպանությունն իրականացվում է ստացող Կողմի պետության ազգային օրենսդրության և (կամ) համապատասխան նորմատիվ իրավական ակտերին համապատասխան: Այդպիսի տեղեկատվությունը չի բացահայտվում և չի փոխանցվում երրորդ անձանց և կողմերի՝ առանց այդ տեղեկատվությունը տրամադրած Կողմի գրավոր համաձայնության և պայմանների պահպանման:

Այդպիսի տեղեկատվությունը նշագրվում է Կողմերի պետությունների ազգային օրենսդրության և միջազգային պայմանագրերին համապատասխան, իսկ Կողմերի միջև դրա փոխանցման փաստերն արձանագրվում են փաստաթղթերով:

Անձնական տվյալներ պարունակող տեղեկատվության փոխանցումը սույն Համաձայնագրի շրջանակներում իրականացվում է Կողմերի պետությունների ազգային օրենսդրության համապատասխան: Ընդ որում՝ ստացված անձնական տվյալները չեն կարող փոխանցվել երրորդ անձանց և

կողմերին կամ հրապարակվել՝ առանց նշված անձնական տվյալները տրամադրած Կողմի գրավոր համաձայնության:

Հայաստանի Հանրապետության պետական ու ծառայողական գաղտնիք և (կամ) Ռուսաստանի Դաշնության պետական գաղտնիք կազմող տեղեկություններ պարունակող տեղեկատվության փոխանակման կարգը, պայմանները և պաշտպանության միջոցները սույն Համաձայնագրի իրագործման ընթացքում և դրա գործողության ավարտից հետո սահմանվում են «Հայաստանի Հանրապետության կառավարության և Ռուսաստանի Դաշնության կառավարության միջև գաղտնի տեղեկատվության փոխադարձ պաշտպանության մասին» 2002թ. նոյեմբերի 5-ի համաձայնագրով:

Հոդված 7
Ֆինանսավորումը

1. Կողմերն իրենք են կատարում սույն Համաձայնագրի իրականացման նպատակով համապատասխան միջոցառումներին իրենց ներկայացուցիչների և փորձագետների մասնակցության հետ կապված ծախսերը:

2. Սույն Համաձայնագրի կատարման հետ կապված այլ ծախսերի առնչությամբ Կողմերը կարող են յուրաքանչյուր առանձին դեպքում համաձայնեցնել ֆինանսավորման այլ կարգ՝ Կողմերի պետությունների ազգային օրենսդրության համապատասխան:

Հոդված 8
Վեճերի լուծումը

Վիճելի հարցերը, որոնք կարող են ծագել սույն Համաձայնագրի դրույթների մեկնաբանման կամ կիրառման հետ կապված, Կողմերը

կարգավորում են Կողմերի պետությունների իրավասու մարմինների խորհրդակցությունների և բանակցությունների միջոցով, անհրաժեշտության դեպքում՝ դիվանագիտական ուղիներով:

Հոդված 9

Եզրափակիչ դրույթներ

1. Սույն Համաձայնագիրը կնքվում է անժամկետ և ուժի մեջ է մտնում Համաձայնագրի ուժի մեջ մտնելու համար անհրաժեշտ ներպետական ընթացակարգերը Կողմերի կողմից կատարվելու մասին վերջին գրավոր ծանուցումը դիվանագիտական ուղիներով ստանալու օրվանից հետո՝ 30-րդ օրը:

2. Կողմերի համաձայնությամբ սույն Համաձայնագրում կարող են կատարվել սույն Համաձայնագրի անբաժանելի մաս կազմող և առանձին արձանագրություններով ձևակերպվող փոփոխություններ:

3. Սույն Համաձայնագրի գործողությունը կարող է դադարեցվել սույն Համաձայնագիրը դադարեցնելու մտադրության մասին Կողմերից մեկի գրավոր ծանուցումը դիվանագիտական ուղիներով մյուս Կողմի ստանալու օրվանից 90 օրը լրանալուց հետո:

4. Սույն Համաձայնագրի գործողության դադարեցման դեպքում Կողմերը միջոցներ են ձեռնարկում տեղեկատվության պաշտպանության մասով իրենց պարտավորություններն ամբողջությամբ կատարելու համար, ինչպես նաև ապահովում են նախապես համաձայնեցված համատեղ աշխատանքների, նախագծերի և այլ միջոցառումների կատարումը, որոնք իրականացվում են սույն Համաձայնագրի շրջանակներում և ավարտված չեն սույն Համաձայնագրի գործողության դադարեցման պահին:

Կատարված է Մոսկվա քաղաքում, 2022 թվականի սեպտեմբերի «19» -ին, երկու օրինակով, յուրաքանչյուրը՝ հայերեն և ռուսերեն, ընդ որում՝ երկու տեքստերն էլ հավասարազոր են:

Հայաստանի Հանրապետության
կառավարության կողմից՝

Ռուսաստանի Դաշնության
կառավարության կողմից՝

СОГЛАШЕНИЕ

между Правительством Республики Армения и Правительством Российской Федерации о сотрудничестве в области обеспечения информационной безопасности

Правительство Республики Армения и Правительство Российской Федерации, далее именуемые Сторонами,

отмечая значительный прогресс в развитии и внедрении информационно-коммуникационных технологий, оказывающих существенное влияние на обеспечение международной информационной безопасности,

руководствуясь Договором о дружбе, сотрудничестве и взаимной помощи между Республикой Армения и Российской Федерацией от 29 августа 1997 г.,

отмечая большое значение информационно-коммуникационных технологий для социально-экономического развития на благо человечества, а также для поддержания международного мира, безопасности и стабильности,

выражая озабоченность угрозами, связанными с возможностями использования информационно-коммуникационных технологий в целях, несовместимых с задачами обеспечения международного мира, безопасности и стабильности, для подрыва суверенитета и безопасности государств и вмешательства в их внутренние дела, дестабилизации внутриполитической и социально-экономической обстановки, разжигания межнациональной и межконфессиональной вражды,

придавая важное значение международной информационной безопасности как одному из ключевых элементов системы международной безопасности,

поддерживая разработку и принятие под эгидой Организации Объединенных Наций международных правил, норм и принципов ответственного поведения государств в информационном пространстве для содействия обеспечению равной безопасности для всех стран,

подтверждая суверенное право государств определять и проводить государственную политику по вопросам, связанным с информационно-телекоммуникационной сетью "Интернет", включая обеспечение ее безопасного и стабильного функционирования,

будучи убежденными в том, что дальнейшее углубление и развитие взаимодействия Сторон в области использования информационно-коммуникационных технологий отвечают их интересам,

придавая важное значение балансу между обеспечением безопасности и соблюдением прав человека в области использования информационно-коммуникационных технологий в соответствии с национальным законодательством, а также с международными обязательствами государств Сторон,

стремясь предотвратить угрозы международной информационной безопасности и обеспечить национальные интересы в информационной сфере государств Сторон,

желая создать правовые и организационные основы сотрудничества Сторон в области обеспечения информационной безопасности, не направленного против интересов третьей стороны,

согласились о нижеследующем:

Статья 1
Основные угрозы в области обеспечения информационной безопасности

При осуществлении сотрудничества в соответствии с настоящим Соглашением Стороны исходят из того, что основными угрозами в области обеспечения информационной безопасности являются:

1) использование информационно-коммуникационных технологий для осуществления актов, направленных на нарушение суверенитета, безопасности и территориальной целостности государств Сторон;

2) использование информационно-коммуникационных технологий для оказания деструктивного воздействия на объекты критической информационной инфраструктуры;

3) использование информационно-коммуникационных технологий в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности;

4) использование информационно-коммуникационных технологий для совершения преступлений в сфере компьютерной информации, связанных в том числе с неправомерным доступом к компьютерной информации и использованием информационных ресурсов государств Сторон, с созданием, использованием и распространением вредоносных

компьютерных программ, с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, а также в иных преступных целях;

5) использование информационно-коммуникационных технологий для вмешательства во внутренние дела государств Сторон, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей и теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию и нестабильности, а также для дестабилизации внутриполитической и социально-экономической обстановки, нарушения управления государством;

6) использование информационно-коммуникационных технологий для распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной средам государств Сторон.

Статья 2
Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество в области обеспечения информационной безопасности в рамках настоящего Соглашения таким образом, чтобы указанное сотрудничество способствовало социальному и экономическому развитию, было совместимо с задачами поддержания международного мира, безопасности и стабильности и соответствовало общепризнанным принципам и нормам международного права, а также принципам двустороннего сотрудничества и невмешательства в информационные ресурсы государств Сторон.

2. Деятельность Сторон в рамках настоящего Соглашения осуществляется в соответствии с национальным законодательством государств Сторон.

3. Каждая Сторона имеет равные права на защиту информационных ресурсов своего государства от неправомерного использования и несанкционированного вмешательства, в том числе от компьютерных атак на них. Каждая Сторона не осуществляет по отношению к другой Стороне подобных действий и оказывает содействие другой Стороне в реализации указанных прав.

4. Стороны прилагают усилия к тому, чтобы информационная инфраструктура и ресурсы государств Сторон не использовались третьей стороной для нанесения ущерба государствам Сторон.

Статья 3
Основные направления сотрудничества

1. В рамках настоящего Соглашения компетентные органы государств Сторон, которые определяются в соответствии со статьей 5 настоящего Соглашения, осуществляют сотрудничество в области обеспечения информационной безопасности по следующим основным направлениям:

1) координация противодействия угрозам в области обеспечения информационной безопасности, указанным в статье 1 настоящего Соглашения;

2) обмен информацией в правоохранительной области в целях выявления, предупреждения, пресечения и расследования правонарушений, связанных с использованием информационно-коммуникационных технологий в террористических и иных преступных целях;

3) согласование и осуществление необходимых мер доверия, способствующих обеспечению информационной безопасности;

4) обмен информацией между компетентными органами государств Сторон по вопросам обеспечения информационной безопасности, включая сотрудничество в области реагирования на компьютерные инциденты;

5) обмен информацией о законодательстве государств Сторон по вопросам обеспечения информационной безопасности;

6) совершенствование двусторонней нормативно-правовой базы и практических механизмов сотрудничества государств Сторон в области обеспечения информационной безопасности;

7) участие в разработке и продвижении норм международного права в целях обеспечения национальной и международной информационной безопасности;

8) взаимодействие и координация деятельности государств Сторон при решении проблем обеспечения международной информационной безопасности в рамках международных организаций и форумов (включая Организацию Объединенных Наций, Международный союз электросвязи, Организацию по безопасности и сотрудничеству в Европе, Организацию Договора о коллективной безопасности, Содружество Независимых Государств и другие);

9) проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов государств Сторон в сфере информационной безопасности;

10) взаимодействие в области подготовки кадров, стажировок, обмена специалистами в сфере информационной безопасности;

11) обмен опытом по совершенствованию законодательства в области информационной безопасности;

12) содействие осуществлению научно-исследовательской деятельности по вопросам обеспечения информационной безопасности.

2. Стороны или компетентные органы государств Сторон могут определять другие направления сотрудничества путем письменной договоренности.

Статья 4
Координирующие органы

В целях содействия эффективной реализации положений настоящего Соглашения и установления непосредственного взаимодействия между Республикой Армения и Российской Федерацией в рамках настоящего Соглашения координирующими органами определены:

от Республики Армения - Аппарат Совета Безопасности Республики Армения;

от Российской Федерации - Аппарат Совета Безопасности Российской Федерации.

При необходимости Стороны могут заменить координирующий орган, незамедлительно оповестив в письменной форме о таких изменениях другую Сторону по дипломатическим каналам.

Статья 5
Формы и механизмы сотрудничества

1. Практическое взаимодействие по конкретным направлениям сотрудничества, предусмотренным настоящим Соглашением, Стороны могут осуществлять по линии компетентных органов государств Сторон, ответственных за реализацию настоящего Соглашения. В течение 60 дней со дня вступления настоящего Соглашения в силу Стороны обменяются по дипломатическим каналам данными о компетентных органах государств Сторон, ответственных за реализацию настоящего Соглашения.

2. В целях создания правовых и организационных основ сотрудничества по конкретным направлениям компетентные органы государств Сторон могут заключать соответствующие договоры.

3. С целью рассмотрения хода реализации настоящего Соглашения, обмена информацией, анализа и совместной оценки возникающих угроз информационной безопасности, определения, согласования и координации совместных мер реагирования на такие угрозы Стороны проводят на регулярной основе межведомственные консультации с участием представителей компетентных органов государств Сторон, а также консультации компетентных органов государств Сторон.

Межведомственные консультации проводятся по согласованию Сторон не реже одного раза в год попеременно в Республике Армения и Российской Федерации, консультации компетентных органов - по согласованию данных органов.

Каждая из Сторон может инициировать проведение дополнительных консультаций, предлагая время и место их проведения, а также повестку дня.

Статья 6
Защита информации

Стороны обеспечивают надлежащую защиту передаваемой или создаваемой в ходе сотрудничества в рамках настоящего Соглашения информации, доступ к которой ограничен в соответствии с национальным законодательством государств Сторон.

Защита такой информации осуществляется в соответствии с национальным законодательством и (или) соответствующими нормативными правовыми актами государства получающей Стороны. Такая информация не раскрывается и не передается третьим лицам и сторонам без письменного согласия и соблюдения условий предоставившей эту информацию Стороны.

Такая информация обозначается в соответствии с национальным законодательством и международными договорами государств Сторон, а факты ее передачи между Сторонами фиксируются документально.

Передача в рамках настоящего Соглашения информации, содержащей персональные данные, осуществляется в соответствии с национальным законодательством государств Сторон. При этом полученные персональные данные не могут быть переданы третьим лицам

и сторонам либо опубликованы без письменного согласия Стороны, предоставившей указанные персональные данные.

Порядок обмена, условия и меры по защите информации, содержащей сведения, составляющие государственную тайну и служебную тайну Республики Армения и (или) государственную тайну Российской Федерации, в ходе реализации и по окончании действия настоящего Соглашения определяются Соглашением между Правительством Республики Армения и Правительством Российской Федерации о взаимной защите секретной информации от 5 ноября 2002 г.

Статья 7
Финансирование

1. Стороны самостоятельно несут расходы, связанные с участием их представителей и экспертов в соответствующих мероприятиях по выполнению настоящего Соглашения.

2. В отношении прочих расходов, связанных с выполнением настоящего Соглашения, Стороны в каждом отдельном случае могут согласовывать иной порядок финансирования в соответствии с национальным законодательством государств Сторон.

Статья 8
Разрешение споров

Стороны решают спорные вопросы, которые могут возникнуть в связи с толкованием или применением положений настоящего Соглашения, путем консультаций и переговоров между компетентными органами государств Сторон и в случае необходимости по дипломатическим каналам.

Статья 9
Заключительные положения

1. Настоящее Соглашение заключается на неопределенный срок и вступает в силу на 30-й день со дня получения по дипломатическим каналам последнего письменного уведомления о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу.

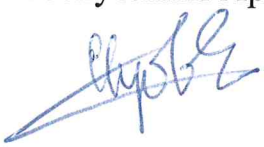
2. По согласию Сторон в настоящее Соглашение могут вноситься изменения, являющиеся неотъемлемой частью настоящего Соглашения и оформляемые отдельными протоколами.

3. Действие настоящего Соглашения может быть прекращено по истечении 90 дней со дня получения одной из Сторон по дипломатическим каналам письменного уведомления другой Стороны о ее намерении прекратить действие настоящего Соглашения.

4. В случае прекращения действия настоящего Соглашения Стороны принимают меры для полного выполнения обязательств по защите информации, а также обеспечивают выполнение ранее согласованных совместных работ, проектов и иных мероприятий, осуществляемых в рамках настоящего Соглашения и не завершенных к моменту прекращения действия настоящего Соглашения.

Совершено в г. Москва, "19" апреля 2022 г. в двух экземплярах, каждый на армянском и русском языках, причем оба текста имеют одинаковую силу.

За Правительство
Республики Армения



За Правительство
Российской Федерации

Սույնով հավաստվում է, որ կցված տեքստը 2022 թվականի ապրիլի 19-ին ստորագրված «Հայաստանի Հանրապետության կառավարության և Ռուսաստանի Դաշնության կառավարության միջև տեղեկատվական անվտանգության ապահովման բնագավառում համագործակցության մասին» համաձայնագրի՝ Հայաստանի Հանրապետության արտաքին գործերի նախարարության միջազգային պայմանագրերի պահոցում (դեպոզիտում) պահվող բնօրինակի նույնական պատճենն է:

Հայաստանի Հանրապետության
արտաքին գործերի նախարարության
միջազգային պայմանագրերի և
իրավունքի վարչության պետի պաշտոնակատար՝

Վահագն Փիլիպոսյան