БЯСПЕКІ РЭСПУБЛІКІ БЕЛАРУСЬ

ў інфармацыйнай сферы з'яўляюцца інфармацыйнае проціборства паміж вядучымі сусветнымі цэнтрамі сілы, мэтанакіраванае фарміраванне ўнутры і за межамі краіны інфармацыйных падстаў для дыскрэдытацыі дзяржаўнай знешняй і ўнутранай палітыкі.

43. З улікам гэтага галоўная мэта забеспячэння бяспекі інфармацыйна-псіхалагічнай кампаненты інфармацыйнай сферы заключаецца ў захаванні інфармацыйнага суверэнітэту і правядзенні палітыкі інфармацыйнага нейтралітэту, а таксама фарміраванні ўстойлівага імунітэту супраць дэструктыўных інфармацыйна-псіхалагічных уздзеянняў на масавую грамадскую свядомасць, а ў неабходных выпадках — і супрацьдзеянне ім.

44. Для гэтага галоўным чынам неабходна на дзяржаўным узроўні забяспечыць фарміраванне, выкарыстанне і развіццё інфармацыйнай прасторы выключна ў мэтах сацыяльнага, эканамічнага і культурнага развіцця, а таксама пастаянную, актыўную і эфектыўную дзейнасць дзяржаўных органаў, арганізацый, навукова-экспертнай супольнасці ў інфармацыйнай прасторы, асабліва нарошчваць яе ў сетцы Інтэрнэт.

45. У прыярытэтным парадку неабходна падтрымліваць захаванне ў грамадстве традыцыйных сацыяльных асноў і каштоўнасцяў, адкрытае і ўсебаковае інфармацыйнае забеспячэнне і суправаджэнне дзяржаўнай палітыкі, а таксама перашкоду ў законным парадку распаўсюджванню незаконнай і недакладнай масавай інфармацыі.

ГЛАВА 12

Захаванне традыцыйных асноў і каштоўнасцяў

46. Для павышэння ўстойлівасці грамадства да дэструктыўных інфармацыйных уздзеянняў неабходна засяродзіць намаганні на захаванні сфарміраваных у грамадскай свядомасці традыцыйных фундаментальных каштоўнасцяў народа, якія выступаюць у якасці аднаго з асноўных элементаў забеспячэння яго адзінства і адной з умоў няўхільнага развіцця дзяржавы.

47. Інфармацыйная палітыка Рэспублікі Беларусь нацэльваецца на прасоўванне такіх жыццёвых прыярытэтаў, як гуманізм, міралюбнасць, добрасуседства, справядлівасць, узаемадапамога, моцныя сямейныя адносіны, здаровы лад жыцця, стваральная праца, прынятыя ў беларускім грамадстве нормы маралі, пазітыўная правасвядомасць. У інфармацыйнай сферы ў поўнай меры знаходзяць адлюстраванне роўныя правы ўсіх без выключэння нацыянальнасцяў, якія насяляюць Рэспубліку Беларусь, паважлівае стаўленне да ўсіх традыцыйных рэлігій і веравызнанняў. Найважнейшае значэнне мае падтрымка і ўсямернае развіццё грамадзянска-патрыятычнай ідэалогіі.

48. Беларуская мова разам з канстытуцыйна замацаваным у дзяржаве двухмоўем садзейнічае павышэнню нацыянальнай самасвядомасці беларускага грамадства і фарміраванню яго духоўнасці. Пашырэнне сацыяльных функцый і камунікатыўных магчымасцяў беларускай мовы, яе паўнавартаснае і ўсебаковае развіццё разам з іншымі элементамі нацыянальнай культуры выступаюць гарантам гуманітарнай бяспекі дзяржавы.

49. Патрабуе далейшай паслядоўнай рэалізацыі дзяржаўная гістарычная палітыка, накіраваная на замацаванне ў Беларусі і за яе межамі беларускай нацыянальнай канцэпцыі гістарычнага мінулага краіны і беларускай мадэлі памяці, пабудаванай у адпаведнасці з гэтай Канцэпцыяй у якасці дамінуючай.

ГЛАВА 13

Інфармацыйнае забеспячэнне і суправаджэнне дзяржаўнай палітыкі

50. Інфармацыйнае забеспячэнне і суправаджэнне дзяржаўнай палітыкі накіравана на развіццё масавай палітычнай свядомасці грамадзян, павышэнне патэнцыялу і якасці дзяржаўнага кіравання, узмацненне ўспрымання Беларусі ў сусветнай інфармацыйнай прасторы. Гэтая дзейнасць ажыццяўляецца праз максімальна адкрытае і аператыўнае давядзенне да насельніцтва Рэспублікі Беларусь і сусветнай супольнасці дакладнай і поўнай інфармацыі аб дзейнасці органаў дзяржаўнай улады Беларусі, мерах, што ажыццяўляюцца па ўдасканаленні сацыяльна-эканамічных адносін, выпрацаваных і прынятых заканадаўчых, іншых нарматыўных прававых актах і іншых рашэннях ва ўнутры- і знешнепалітычнай сферах.

51. Дзяржава забяспечвае пабудову канструктыўнага і ўсёабдымнага інфармацыйнага ўзаемадзеяння паміж органамі ўлады, сродкамі масавай інфармацыі і грамадскасцю на ўсіх узроўнях.

52. Асаблівае значэнне набывае канкурэнтаздольнасць дзяржаўных сродкаў масавай інфармацыі, якая дасягаецца ў тым ліку праз нацыянальную вытворчасць высакаякаснага кантэнту і фарміраванне сучаснай сістэмы медыявымярэнняў.

53. Дзяржава аказвае прававую падтрымку айчынным СМІ, накіраваную на павышэнне якасці аўдыявізуальнага прадукту і пашырэнне тэматычнай і жанравай разнастайнасці праграм, фарміраванне іншых дадатковых магчымасцяў развіцця, у тым ліку праз заканадаўчае рэгламентаванне аб'ёму і якасці замежнага вяшчання ў Рэспубліцы Беларусь, рэгуляванне аб'ёму рэкламных паслуг, вызначэнне аптымальных умоў рэгістрацыі.

54. Органы ўлады, іншыя дзяржаўныя органы і арганізацыі, установы навукі, адукацыі і культуры, службовыя асобы і прадстаўнікі навукова-экспертнай супольнасці праводзяць актыўную, высокатэхналагічную і рознабаковую дзейнасць у інфармацыйнай прасторы, уключаючы нацыянальныя і замежныя электронныя сродкі масавай інфармацыі, іншыя інтэрнэт-рэсурсы і сродкі інтэрнэт-камунікацыі, а таксама ствараюць умовы для фарміравання сучасных айчынных медыйных аналітычных, навуковых і дыскусійных пляцовак.

ГЛАВА 14

Бяспека масавай інфармацыі

55. Адносіны ў галіне масавай інфармацыі заснаваны на прынцыпах законнасці, дакладнасці, павагі правоў і свабод чалавека, разнастайнасці думак, абароны маралі і іншых. Нароўні з канстытуцыйным забеспячэннем свабоды слова ў Рэспубліцы Беларусь для захавання гэтых прынцыпаў усталёўваюцца заканадаўчыя патрабаванні да распаўсюджвання масавай інфармацыі, якія адпавядаюць сусветнай практыцы і агульнапрынятым сацыяльным стандартам. Ажыццяўляецца грамадскі кантроль за распаўсюджваннем у інфармацыйнай прасторы незаконнай і недакладнай інфармацыі.

56. Не дапускаецца распаўсюджванне інфармацыі, якая накіравана на прапаганду вайны, экстрэмісцкай дзейнасці або змяшчае заклікі да такой дзейнасці, ужывання наркатычных сродкаў і ім падобных рэчываў, парнаграфіі, гвалту і жорсткасці, іншай інфармацыі, забароненай заканадаўствам. На дзяржаўным узроўні рэалізуюцца меры па перашкодзе распаўсюджванню інфармацыі, здольнай нанесці шкоду нацыянальным інтарэсам, і недакладных звестак, а таксама па зніжэнні ананімнасці ў інфармацыйнай прасторы. Пры трансляцыі кантэнту не дазваляецца прымяненне схаваных тэхналагічных прыёмаў, якія ўздзейнічаюць на падсвядомасць людзей або аказваюць шкодны ўплыў на іх здароўе.

57. Абмяжоўваецца ў заканадаўчым парадку распаўсюджванне інфармацыі без знака ўзроставай катэгорыі, а таксама заахвочваюцца меры бацькоўскага кантролю пры выкарыстанні дзецьмі інфармацыйных тэхналогій.

РАЗДЗЕЛ V
ЗАБЕСПЯЧЭННЕ БЯСПЕКІ ІНФАРМАЦЫЙНАЙ ІНФРАСТРУКТУРЫ

ГЛАВА 15

Абумоўленасць мер па забеспячэнні бяспекі інфармацыйнай інфраструктуры

58. Лічбавая трансфармацыя эканомікі і інавацыі ў галіне ІКТ нароўні з сусветным развіццём і нарошчваннем тэхналагічных магчымасцяў ва ўзаемадзеянні людзей, бізнесу, дзяржаўных інстытутаў абумоўліваюць неабходнасць прыняцця асобых мер, якія гарантуюць давер і бяспеку пры стварэнні і выкарыстанні ў сучасным інфармацыйным грамадстве інфармацыйнай інфраструктуры і даных у інфармацыйных сістэмах.

59. Палітычная і сацыяльна-эканамічная сферы, грамадская і ваенная бяспека становяцца ўсё больш уразлівымі перад наўмыснымі або выпадковымі тэхналагічнымі ўздзеяннямі, якія фарміруюцца ў тым ліку ва ўмовах недастатковых глабальных механізмаў узгодненага і дзейснага папярэджання і стрымлівання кіберінцыдэнтаў у сетцы Інтэрнэт.

Паўсюднае функцыянаванне аб'ектаў прамысловасці, транспарту, энергетыкі, электрасувязі, аховы здароўя і сістэм жыццезабеспячэння з аўтаматызаванымі сістэмамі кіравання ставіць у прамую залежнасць жыццё і здароўе насельніцтва, экалагічную і сацыяльную бяспеку ад іх надзейнасці і абароненасці. Кібератакі на інфармацыйную інфраструктуру разглядаюцца ў свеце як адна з найбольш значных пагроз бяспецы.

У многіх нацыянальных узброеных сілах ствараюцца і развіваюцца кібервойскі, а правядзенне кібераперацый прадугледжваецца ў дактрынальных і стратэгічных дакументах. Адначасова разглядаецца магчымасць рэагавання на кібератакі як на ўзброеную агрэсію, што ва ўмовах практычнай немагчымасці дакладнай ідэнтыфікацыі іх крыніц (ініцыятараў) можа прывесці да бяздоказнай і адвольнай трактоўкі абгрунтаванасці сустрэчных ваенных дзеянняў.

Няўхільна расце колькасць кіберзлачынстваў. Інфармацыйныя сістэмы і рэсурсы становяцца як прадметам злачынстваў, так і сродкам іх здзяйснення. Фарміруецца татальная залежнасць фінансавага сектара і іншых сектараў ад надзейнасці электронных сістэм захавання, апрацоўкі і абмену данымі.

60. Аднак ні ў глабальным, ні ў рэгіянальных маштабах пакуль не ўдаецца эфектыўна перашкодзіць распрацоўкам і распаўсюджванню сродкаў, заведама прызначаных для знішчэння, блакіравання, мадыфікацыі, выкрадання інфармацыі ў сетках і рэсурсах або нейтралізацыі мер па яе абароне. Выпрацоўка прававых, працэдурных, тэхнічных і арганізацыйных мер супраць кіберуздзеянняў на інфармацыйныя рэсурсы адстае ад фарміравання рэальных і патэнцыйных пагроз іх ажыццяўлення.

ГЛАВА 16

Асноўныя кірункі забеспячэння бяспекі інфармацыйнай інфраструктуры

61. У якасці найбольш верагодных крыніц пагроз кібербяспецы разглядаюцца адмовы тэхнічных сродкаў і збоі праграмнага забеспячэння ў інфармацыйных і тэлекамунікацыйных сістэмах, супрацьпраўная дзейнасць асобных асоб і злачынных груп, наўмысныя дзеянні і памылкі персаналу інфармацыйных сістэм, якія выяўляюцца ў парушэнні ўстаноўленых рэгламентаў іх эксплуатацыі і правілаў апрацоўкі інфармацыі, залежнасць Беларусі ад іншых краін — вытворцаў праграмных і апаратных сродкаў пры стварэнні і развіцці інфармацыйнай інфраструктуры.

62. Перад Рэспублікай Беларусь стаіць стратэгічная мэта развіцця сістэмы забеспячэння кібербяспекі, якая базіруецца на перадавых міжнародных падыходах кіравання рызыкамі і прызначана для рэалізацыі доўгатэрміновых мер па іх скарачэнні да прымальнага ўзроўню.

63. Нацыянальная сістэма забеспячэння кібербяспекі павінна рэалізоўваць увесь магчымы комплекс прававых, арганізацыйных і тэхнічных мер па забеспячэнні бяспекі нацыянальнай інфармацыйнай інфраструктуры, у тым ліку інфармацыйных сістэм, забяспечваць канфідэнцыяльнасць, даступнасць і цэласнасць інфармацыі, а таксама лёгка трансфармавацца і адаптавацца ў зменлівай абстаноўцы за кошт пастаяннага аналізу на прадмет адпаведнасці актуальным рызыкам кібербяспекі.

64. У першую чаргу неабходна забяспечыць кіберустойлівасць нацыянальнага сегмента сеткі Інтэрнэт, крытычна важных аб'ектаў інфарматызацыі і дзяржаўных інфармацыйных сістэм, эфектыўнае процідзеянне кіберзлачынствам.

ГЛАВА 17

Бяспека нацыянальнага сегмента сеткі Інтэрнэт

65. Неабходнай умовай рэалізацыі правоў грамадзян у інфармацыйнай сферы, падтрымання высокага ўзроўню інфармацыйнага абмену, аказання інфармацыйных паслуг з'яўляецца ўстойлівае функцыянаванне і кіравальнасць нацыянальнага сегмента сеткі Інтэрнэт. У Рэспубліцы Беларусь кібербяспека нацыянальнага сегмента сеткі Інтэрнэт забяспечваецца галоўным чынам за кошт адбіцця асноўнага аб'ёму кібератак на інфармацыйныя сістэмы і сеткі перадачы даных шляхам блакіравання шкодных камунікацый паміж суб'ектамі і аб'ектамі ўздзеянняў.

66. Дзяржавай падтрымліваецца і стымулюецца прымяненне найлепшых практык забеспячэння кібербяспекі. Найбольш перспектыўнай задачай разглядаецца стварэнне адзінай дзяржаўнай сістэмы маніторынгу нацыянальнага сегмента сеткі Інтэрнэт з адначасовым фарміраванем воблачнай платформы прадастаўлення комплексных сэрвісаў інфармацыйнай бяспекі дзяржаўнаму сектару і бізнес-супольнасці ў інтарэсах аўтаматызаванага ўліку кіберінцыдэнтаў і аператыўнага абмену інфармацыяй аб іх паміж упаўнаважанымі дзяржаўнымі органамі, аператарамі электрасувязі і камандамі хуткага рэагавання на камп'ютарныя інцыдэнты (CERT/CSIRT). У перспектыве таксама неабходна фарміраванне экасістэмы для стварэння і функцыянавання нацыянальнага цэнтра сведчання, каранёвы сертыфікат якога будзе з'яўляцца даверaным для асноўных аперацыйных сістэм і вэб-браўзераў.

67. Разам з гэтым трэба арганізаваць функцыянаванне службы ацэнкі рэпутацыі IP-адрасоў для прадастаўлення ў рэжыме рэальнага часу пастаўшчыкам інтэрнэт-паслуг звестак аб адрасах, якія выкарыстоўваюцца для кібератак.

68. Неабходна забяспечыць дасягненне і захаванне балансу паміж надзейнай ідэнтыфікацыяй карыстальнікаў, рэгістрацыяй іх дзеянняў і стварэннем умоў для бяспечнага збору, апрацоўкі, прадастаўлення, захавання і распаўсюджвання персанальных даных у нацыянальным сегменце сеткі Інтэрнэт, а таксама фарміраванне і развіццё нацыянальных рынкаў страхавання кіберрызык і паслуг тэсціравання на пранікненне.

ГЛАВА 18

Кіберустойлівасць КВАІ і дзяржаўных інфармацыйных сістэм

69. Забеспячэнне бяспекі інфармацыйнай інфраструктуры ажыццяўляецца шляхам выдзялення найбольш значных аб'ектаў інфарматызацыі, адмова функцыянавання або парушэнне работы якіх можа пацягнуць значныя негатыўныя наступствы для нацыянальнай бяспекі ў палітычнай, эканамічнай, сацыяльнай, інфармацыйнай, экалагічнай і іншых сферах.

З мэтай дасягнення кіберустойлівасці КВАІ ў Рэспубліцы Беларусь рэалізуецца асобы комплекс прававых, арганізацыйных і тэхнічных мерапрыемстваў, заснаваны на выпрацоўцы крытэрыяў аднясення аб'ектаў да такой катэгорыі і прыняцці ў дачыненні да іх адпаведных мэтанакіраваных і ўсебаковых ахоўных мер. Такі падыход дазваляе ствараць індывідуальную мадэль бяспекі кожнага КВАІ з улікам сістэматызаваных агульных патрабаванняў па бяспецы, эфектыўна выяўляць і ацэньваць рызыкі, падтрымліваць высокую гатоўнасць да папярэджання і лакалізацыі наступстваў кібератак, а таксама праводзіць знешнюю ацэнку створаных сістэм бяспекі.

70. Павышэнне эфектыўнасці забеспячэння бяспекі КВАІ неабходна ажыццяўляць з дапамогай інтэгравання ў дзяржаўную сістэму маніторынгу нацыянальнага сегмента сеткі Інтэрнэт галіновых сістэм маніторынгу і кантролю кіберпагроз. Пры забеспячэнні кіберустойлівасці КВАІ Беларусь зацікаўлена ў выкарыстанні міжнародных стандартаў і найлепшых практык. Важнае практычнае значэнне маюць рэгулярныя кібервучэнні і спаборніцтвы з прыцягненнем эксплуатуючага персаналу, уласнікаў, уладальнікаў і знешніх суб'ектаў, якія задзейнічаны ў гарантаванні кібербяспекі.

71. Дзяржава зацікаўлена ў абароне ад рызык, выклікаў і пагроз дзяржаўных інфармацыйных сістэм. У гэтых мэтах вызначаюцца парадак іх стварэння і эксплуатацыі, уключэння ў інфармацыйныя сеткі і правілы абмену інфармацыяй, а таксама прымяняюцца спецыяльныя працэдуры дзяржаўнай рэгістрацыі.

У перспектыве дасягненне неабходнага ўзроўню абароны сэрвісаў электроннага ўрада і кіберустойлівасці дзяржаўных інфармацыйных сістэм павінна забяспечвацца галоўным чынам за кошт іх бяспечнага праектавання і эксплуатацыі, а не прыняцця далейшых ахоўных мер, а таксама праз укараненне іх абгрунтаванай уніфікацыі пры пабудове і мадэрнізацыі гэтых сістэм.

72. Неад'емнай часткай забеспячэння бяспекі КВАІ і дзяржаўных інфармацыйных сістэм з'яўляецца выкарыстанне арыгінальнага ліцэнзійнага праграмнага забеспячэння, якое рэгулярна абнаўляецца і атрымліваецца з даверaных крыніц.

ГЛАВА 19

Процідзеянне кіберзлачыннасці

73. У Рэспубліцы Беларусь створана сістэма папярэджання, выяўлення, спынення і ўсебаковага расследавання кіберзлачынстваў. Забяспечваецца адпаведнасць нормаў Крымінальнага кодэкса Рэспублікі Беларусь у гэтай галіне ўзроўню грамадскага развіцця, сусветным тэндэнцыям прававога рэгулявання і перадавому замежнаму вопыту.

У сувязі са з'яўленнем новых грамадска небяспечных дзеянняў у інфармацыйнай сферы вызначаецца крымінальная і іншая адказнасць за іх здзяйсненне. Забяспечваецца пастаяннае ўдасканаленне формаў і метадаў папярэджання, выяўлення, спынення і расследавання кіберзлачынстваў, павышаецца своечасовасць і якасць аператыўна-вышуковай дзейнасці.

74. Беларусь зацікаўленая ў збліжэнні і ўніфікацыі падыходаў процідзеяння кіберзлачынствам на міжнародным узроўні, выпрацоўцы агульных стандартаў у правапрымяняльнай практыцы, міжнародным абмене вопытам і практычным узаемадзеянні. Ажыццяўляюцца рэалізацыя рэгіянальнага і міжнароднага супрацоўніцтва ў сферы кібербяспекі, адсочванне дзейнасці злачынных груп і асобных злачынцаў, якія дзейнічаюць у кіберпрасторы.

75. Важнае значэнне ў супрацьдзеянні кіберзлачынствам мае павышэнне даверу паміж праваахоўнымі органамі, арганізацыямі дзяржаўнага і прыватнага сектараў, адукацыйнымі і навуковымі ўстановамі, аб'яднанне іх намаганняў у папярэджанні, выяўленні, спыненні і расследаванні кіберзлачынстваў. Адной з эфектыўных мер папярэджання і прафілактыкі кіберзлачынстваў з'яўляецца зніжэнне матывацыі іх здзяйснення за кошт ліквідацыі ўмоў фарміравання супрацьпраўных схем.

(Заканчэнне на 8-й стар.)