КАНЦЭПЦЫЯ ІНФАРМАЦЫЙНАЙ

Для вырашэння гэтай задачы ў краіне вызначаны структура кіравання інфарматызацыяй і архітэктура электроннага ўрада. Развіваюцца інавацыйныя лічбавыя тэхналогіі, заснаваныя на сістэмах штучнага інтэлекту, нейронных сетак, якія забяспечваюць работу з разнастайнымі інфармацыйнымі рэсурсамі, у тым ліку масівамі вялікіх даных, метадах размеркаваных вылічэнняў (воблачныя тэхналогіі), тэхналогіі рэестра блокаў транзакцый (блакчэйн).

Беларусь паслядоўна ўдзельнічае ў працэсах інфарматызацыі на трансгранічным контуры, у тым ліку ў рамках Саюзнай дзяржавы Беларусі і Расіі, Еўразійскага эканамічнага саюза, Садружнасці Незалежных Дзяржаў, Еўрапейскага саюза і іншых сусветных сістэм палітычнага і эканамічнага ўзаемадзеяння і партнёрства.

14. Разам з гэтым аб'ём прымянення інфармацыйных тэхналогій у рэальным сектары эканомікі застаецца невысокім. Ступень лічбавізацыі галін эканомікі розная, што зніжае чаканы сінергетычны эфект ад сінхроннай інфарматызацыі, і з улікам гэтага трэба распрацоўваць лічбавую палітыку для канкрэтных сфер дзяржаўнай жыццядзейнасці, арыентаваць пілотныя праекты лічбавізацыі на іх галіновае маштабаванне, ствараць цэнтры кампетэнцыі па пытаннях лічбавай трансфармацыі. Патрабуецца пераход электроннага ўрада ад простага аказання паслуг па запытах грамадзян да праактыўнай работы з насельніцтвам. Хуткае развіццё ІКТ і павелічэнне інфармацыйных патрэб грамадства абумоўліваюць неабходнасць асваення новых стандартаў у сферы тэлекамунікацый, павышэння прадукцыйнасці і надзейнасці сеткавай інфраструктуры.

РАЗДЗЕЛ III
ДЗЯРЖАЎНАЯ ПАЛІТЫКА ЗАБЕСПЯЧЭННЯ ІНФАРМАЦЫЙНАЙ БЯСПЕКІ

ГЛАВА 6
Мэты і кірункі дзяржаўнай палітыкі

15. Мэтай забеспячэння інфармацыйнай бяспекі з'яўляецца дасягненне і падтрыманне такога ўзроўню абароненасці інфармацыйнай сферы, які забяспечвае рэалізацыю нацыянальных інтарэсаў Рэспублікі Беларусь і яе прагрэсіўнае развіццё.

Забеспячэнне інфармацыйнай бяспекі ажыццяўляецца ў адпаведнасці з дзяржаўнай палітыкай у гэтай галіне, якая ўключае ў сябе фарміраванне, удасканаленне і рэалізацыю арганізацыйных, прававых, навукова-тэхнічных, праваахоўных, эканамічных мер забеспячэння нацыянальнай бяспекі ў інфармацыйнай сферы. У сваю чаргу, менавіта праз развіццё гэтай сферы галоўным чынам гарантуецца і яе бяспека.

16. На дзяржаўным узроўні ажыццяўляецца маніторынг, аналіз і ацэнка стану інфармацыйнай бяспекі, прымяняюцца індыкатары ацэнкі яе стану. Вызначаюцца прыярытэтныя кірункі прадухілення пагроз інфармацыйнай бяспецы, мінімізацыі іх дэструктыўнага ўздзеяння і лакалізацыі наступстваў. Распрацоўваецца і рэалізуецца комплекс мер стратэгічнага і тактычнага характару па папярэджанні і нейтралізацыі інфармацыйных рызык, выклікаў і пагроз.

17. Забяспечваецца канстытуцыйнае права грамадзян свабодна шукаць, атрымліваць, перадаваць, вырабляць, захоўваць і распаўсюджваць інфармацыю любым законным спосабам, права на тайну асабістага жыцця і іншую тайну, што ахоўваецца законам, абарону персанальных даных і аўтарскіх правоў, а таксама захаванне балансу правоў з абмежаваннямі, звязанымі з гарантаваннем нацыянальнай бяспекі. Фарміруюцца прававыя, арганізацыйныя і тэхналагічныя ўмовы для бяспекі функцыянавання нацыянальных сродкаў масавай інфармацыі, ажыццяўляецца дзяржаўны і грамадскі кантроль іх дзейнасці.

(Працяг. Пачатак на 5-й стар.)

Рэалізуецца максімальная даступнасць для грамадзян і арганізацый дзяржаўных электронных паслуг, адміністрацыйных працэдур і інфармацыйных рэсурсаў дзяржаўных органаў і арганізацый.

Павышаецца дасведчанасць грамадзян і грамадства аб пагрозах нацыянальнай бяспецы і дзяржаўных мерах па яе гарантаванні, іх уцягнутасць у забеспячэнне бяспекі інфармацыйнай сферы.

18. Дзяржава ўсебакова садзейнічае абароненасці нацыянальных інфармацыйных сістэм, арганізацыі бяспекі праграмнага забеспячэння, якое выкарыстоўваецца грамадзянамі і арганізацыямі. З мэтай паляпшэння ўстойлівасці дзяржаўнага сектара да інфармацыйных рызык асвойваюцца перадавыя тэхналогіі, укараняюцца новыя сродкі і спосабы забеспячэння інфармацыйнай бяспекі.

Распрацоўваюцца стандарты інфармацыйнай бяспекі і з іх улікам праводзіцца аўдыт дзяржаўных сістэм інфармацыйнай бяспекі. Развіваецца смарт-праектаванне рашэнняў па забеспячэнні інфармацыйнай бяспекі. На нарматыўным узроўні вылучаецца і рэгламентуецца функцыянаванне крытычна важных аб'ектаў інфарматызацыі (далей — КВАІ). Заахвочваецца развіццё тэхналогій бяспекі ў бізнесе і жыццядзейнасці грамадзян.

19. Дзеянні, якія наносяць істотную шкоду інтарэсам, што ахоўваюцца законам, у інфармацыйнай сферы або якія ствараюць небяспеку яе прычынення, крыміналізуюцца ў крымінальным законе ў адпаведнасці з існуючымі сусветнымі падыходамі. Рэалізуюцца крокі па зніжэнні пагроз кіберзлачыннасці, у тым ліку кібертэрарызму, расследаванні і спыненні дзеянняў уцягнутых у тэрарыстычную дзейнасць асоб, перакрыцці каналаў прапаганды тэрарызму, прыцягнення і вярбоўкі прыхільнікаў, заахвочвання і правакавання тэрарыстычнай актыўнасці, фінансавання тэрарызму.

Уводзяцца прававыя рэжымы бяспекі інфармацыі і інфармацыйных рэсурсаў, тэхнічныя ўмовы і палітыкі бяспекі. Ажыццяўляецца выяўленне і прыцягненне да ўстаноўленай законам адказнасці асоб, якія наносяць шкоду дзяржаўным інфармацыйным сістэмам, забяспечваецца дзяржаўная абарона інтарэсаў грамадзян і арганізацый незалежна ад формаў уласнасці.

20. Развіваецца ўзаемадзеянне дзяржавы, грамадскасці, бізнес-супольнасці, СМІ ў мэтах своечасовага выяўлення рызык і выклікаў інфармацыйнай бяспекі, перашкоды кібератакам і акцыям дэструктыўнага інфармацыйнага ўздзеяння, павышэння эфектыўнасці праваахоўнай дзейнасці.

21. Удзяляецца асаблівая ўвага кадраваму патэнцыялу ў забеспячэнні інфармацыйнай бяспекі. На сучасным адукацыйным і тэхналагічным узроўні ажыццяўляецца спецыяльная падрыхтоўка, перападрыхтоўка і павышэнне прафесійнай кваліфікацыі асоб, якія забяспечваюць інфармацыйную бяспеку, супрацоўніцтва паміж дзяржаўнымі органамі, установамі адукацыі і галіновымі прадпрыемствамі ў падборы, падрыхтоўцы і працаўладкаванні такіх кадраў, інтэграванне тэматыкі інфармацыйнай бяспекі ў адукацыйныя праграмы ўсіх узроўняў навучання. Фарміруецца дзяржаўны заказ на падрыхтоўку кадраў.

22. Вырабляюцца сродкі забеспячэння інфармацыйнай бяспекі. Нарошчваецца навуковы патэнцыял і фінансаванне работ па даследаванні і стварэнні новых рашэнняў у сферы забеспячэння інфармацыйнай бяспекі, у тым ліку тэхнічнай абароны інфармацыі, крыптalогіі, крыміналогіі, крыміналістыкі. Дзяржава ажыццяўляе фінансаванне прыярытэтных кірункаў забеспячэння інфармацыйнай бяспекі, перш за ўсё ў рамках дзяржаўных праграм. Распрацоўваюцца інавацыйныя метады і тэхналогіі абароны інфармацыйных рэсурсаў і сістэм.

23. Ажыццяўляюцца намаганні па павышэнні дзейснасці міжнароднага права і захаванні маральных нормаў адказных паводзінаў у інфармацыйнай прасторы, аказваецца садзейнічанне распрацоўцы і ўкараненню мер па ўмацаванні даверу ў інфармацыйнай прасторы. Ствараюцца і развіваюцца каналы міжнароднага абмену вопытам у галіне забеспячэння інфармацыйнай бяспекі, а таксама інфармацыяй аб пагрозах нацыянальным інтарэсам, у тым ліку ўразлівасцях інфармацыйных сістэм, інцыдэнтах у інфармацыйнай інфраструктуры.

24. Бяспека інфармацыйнай сферы і ў цэлым стан інфарматызацыі ў Рэспубліцы Беларусь характарызуюцца міжнароднымі рэйтынгамі і іншымі агульнапрынятымі ў свеце крытэрыямі, індэксамі і індыкатарамі, у тым ліку якія ляжаць у аснове паказчыкаў сацыяльна-эканамічнага развіцця, забеспячэння нацыянальнай бяспекі і адлюстроўваюць іншую ўсебаковую дзейнасць дзяржавы, звязаную з гэтай сферай.

ГЛАВА 7
Інфармацыйны суверэнітэт

25. Ва ўмовах абвастрэння міжнародных супярэчнасцяў становіцца праблематычным выпрацаваць эфектыўныя і агульнапрынятыя правілы паводзінаў сусветнай супольнасці ў інфармацыйнай прасторы. Падыходы розных краін да ацэнкі пагроз у інфармацыйнай сферы і супрацьдзеянні ім не супадаюць, а па асобных кірунках палярызуюцца.

У сувязі з гэтым найважнейшай мэтавай устаноўкай забеспячэння інфармацыйнай бяспекі з'яўляецца інфармацыйны суверэнітэт Рэспублікі Беларусь.

26. Інфармацыйны суверэнітэт дасягаецца, перш за ўсё, шляхам фарміравання сістэмы прававога рэгулявання адносін у інфармацыйнай сферы, якая гарантуе бяспечнае ўстойлівае развіццё, сацыяльную справядлівасць і згоду.

27. У рамках гэтай сістэмы дзяржава забяспечвае развіццё нацыянальных СМІ і тэлекамунікацый, сучасных ІКТ, нацыянальнай індустрыі вытворчасці сродкаў інфарматызацыі, а таксама абарону нацыянальных рынкаў інфармацыйных і тэлекамунікацыйных паслуг, якія зніжаюць залежнасць ад тэхналогій замежнай вытворчасці і скарачаюць лічбавую няроўнасць. У грамадстве выхоўваецца і стымулюецца крытычнае стаўленне да праяў непавагі да нацыянальных асноў, традыцый і парушэнняў нормаў маралі і права ў інфармацыйнай сферы, нецярпімасць да дэзынфармацыі, інфармацыйных маніпуляцый і іншых няяўных інфармацыйна-псіхалагічных уздзеянняў.

28. Фарміруюцца прававыя ўмовы і межы дзейнасці замежных і міжнародных суб'ектаў у нацыянальнай інфармацыйнай прасторы для забеспячэння патрэб грамадзян у знешнім інфармацыйным абмене без культурнай і інфармацыйнай экспансіі, умяшання ва ўнутраныя справы Рэспублікі Беларусь.

29. Ствараюцца неабходныя ўмовы для пабудовы і бяспечнага развіцця функцыянальнай, тэхналагічна самадастатковай, надзейнай і ўстойлівай інфармацыйнай інфраструктуры. Ажыццяўляецца абарона інфармацыйных рэсурсаў, у тым ліку дзяржаўных сакрэтаў, іншай ахоўваемай інфармацыі, персанальных даных, якая забяспечвае палітычную самастойнасць дзяржавы, абароненасць жыццёвай прасторы чалавека, захаванне духоўных і культурных каштоўнасцяў беларускага грамадства, навукова-тэхналагічныя перавагі і рэалізацыю іншых нацыянальных інтарэсаў. Рэспублікай Беларусь рэалізуецца прынцып «суверэнітэту даных».

30. Імкненне да інфармацыйнага суверэнітэту не разыходзіцца з міжнародна-прававымі прынцыпамі забеспячэння правоў і свабод, якія гарантуюць канкурэнтнае і свабоднае развіццё ва ўмовах сусветнай лічбавай трансфармацыі.

ГЛАВА 8
Інфармацыйны нейтралітэт

31. У міжнародных адносінах інфармацыйны суверэнітэт Рэспублікі Беларусь забяспечваецца ў тым ліку на аснове прынцыпу інфармацыйнага нейтралітэту, які прадугледжвае правядзенне міралюбнай знешняй інфармацыйнай палітыкі, павагу агульнапрызнаных і агульнапрынятых правоў любой дзяржавы ў гэтай сферы, выключэнне ініцыятывы ўмяшання ў інфармацыйную сферу іншых краін, накіраванага на дыскрэдытацыю або аспрэчванне іх палітычных, эканамічных, сацыяльных і духоўных стандартаў і прыярытэтаў, а таксама нанясення шкоды інфармацыйнай інфраструктуры якіх бы там ні было дзяржаў і ўдзелу ў іх інфармацыйным супрацьстаянні. Пры гэтым Рэспубліка Беларусь адстойвае ўласныя нацыянальныя інтарэсы ў інфармацыйнай сферы з выкарыстаннем усіх наяўных сіл і сродкаў.

32. У мэтах забеспячэння палітыкі інфармацыйнага нейтралітэту павышаецца ступень прысутнасці Беларусі ў сусветнай інфармацыйнай прасторы, пашыраецца міжнародны інфармацыйны абмен, падтрымліваецца ўстанаўленне і рэгуляванне ўсеагульных правілаў паводзінаў у гэтай сферы і ажыццяўляецца заключэнне пагадненняў па гарантаванні міжнароднай інфармацыйнай бяспекі.

ГЛАВА 9
Дзяржаўнае рэагаванне на рызыкі, выклікі і пагрозы ў інфармацыйнай сферы

33. Дзяржава ажыццяўляе рэагаванне на рызыкі і выклікі ў інфармацыйнай сферы з мэтай папярэджання іх трансфармацыі ў пагрозы нацыянальнай бяспецы, развіцця і маштабавання шкоднага ўздзеяння.

Рэагаванне на рызыкі і выклікі ў інфармацыйнай сферы ажыццяўляецца ўсімі без выключэння дзяржаўнымі органамі і арганізацыямі ў адпаведнасці з галіной іх дзейнасці згодна з непасрэдным прызначэннем максімальна поўна і аператыўна. Дзяржава ў асобе гэтых дзяржаўных органаў і арганізацый забяспечвае своечасовае прыняцце мер бяспекі, неадкладна апавяшчае зацікаўленыя суб'екты, мінімізуе шкоду і лакалізуе наступствы, вызначае датычных асоб і арганізацыі, назапашвае вопыт процідзеяння пагрозам.

34. Дзяржаўнае рэагаванне на рызыкі, выклікі і пагрозы ў інфармацыйнай сферы прадугледжвае збор інфармацыі аб выкарыстоўваемых тэхналогіях, спосабах дэструктыўных інфармацыйных уздзеянняў і здзяйснення кіберзлачынстваў, аналіз, ацэнку і прагназаванне стану бяспекі гэтай сферы, выяўленне выклікаў і пагроз, якія рэалізуюцца, лакалізацыю негатыўных наступстваў і аднаўленне нанесенай шкоды (урону). Вызначаецца абароненасць і ўстойлівасць аб'ектаў інфармацыйнай бяспекі, у тым ліку інфармацыйнай інфраструктуры, інфармацыйных рэсурсаў, індывідуальнай, групавой і масавай свядомасці да дзеяння пагроз. Выяўляюцца і выключаюцца ўмовы ўзнікнення і рэалізацыі рызык, выклікаў і пагроз інфармацыйнай бяспецы.

35. Падрыхтоўваюцца і ўкараняюцца сцэнарыі і планы крызіснага рэагавання на кібератакі, камп'ютарныя інцыдэнты, акты дэструктыўнага інфармацыйнага ўздзеяння, іншыя пагрозы інфармацыйнай бяспецы, а таксама праводзяцца вучэнні і трэніроўкі сіл рэагавання.

Рэалізуецца палітыка інфармацыйнага стрымлівання, якая выяўляецца ў дэманстрацыі дакладнай гатоўнасці да адбіцця дэструктыўных інфармацыйных уздзеянняў, дастатковай магчымасці тэхналагічнага, арганізацыйнага, прававога процідзеяння пагрозам у інфармацыйнай сферы і выяўлення іх крыніц.

36. У выпадку істотнага ўскладнення інфармацыйнай абстаноўкі, звязанага ў тым ліку з неабходнасцю забеспячэння ваеннай бяспекі дзяржавы, ажыццяўляюцца дадатковыя меры абароны інфармацыйнай сферы прававымі, інфармацыйна-тэхналагічнымі, тэхнічнымі і іншымі метадамі (інфармацыйнае процідзеяння), забяспечваецца прыярытэтнае ўзаемадзеянне ваеннай арганізацыі дзяржавы і грамадзянскага сектара.

37. Узброеныя Сілы Рэспублікі Беларусь, іншыя воінскія фарміраванні арганізуюць меры па забеспячэнні інфармацыйнай бяспекі ў рамках рашэння ўскладзеных задач па сваім непасрэдным прызначэнні з прымяненнем сучасных, высокатэхналагічных сіл і сродкаў.

38. Беларусь удзельнічае ў міжнародным рэагаванні на патэнцыяльныя рызыкі, выклікі і пагрозы інфармацыйнай бяспецы ў рамках заключаных дагавораў і пагадненняў, ажыццяўляе міждзяржаўнае ўзаемадзеянне ў аналізе рызык, выклікаў і пагроз інфармацыйнай бяспецы, абмен вопытам і сумесныя практычныя мерапрыемствы.

РАЗДЗЕЛ IV
БЯСПЕКА ІНФАРМАЦЫЙНАЙ ПРАСТОРЫ ЯК АДНА З НАЙВАЖНЕЙШЫХ УМОЎ РАЗВІЦЦЯ СУВЕРЭННАЙ, ДЭМАКРАТЫЧНАЙ САЦЫЯЛЬНАЙ ДЗЯРЖАВЫ

ГЛАВА 10
Абумоўленасць мер па забеспячэнні бяспекі ў інфармацыйнай прасторы

39. Глабальнае ўзрастанне ролі інфармацыі ў сістэме грамадскіх адносін, адкрытасць інфармацыйнай прасторы і павышэнне ўзроўню інфарматызацыі насельніцтва абумоўліваюць новыя меры бяспекі інфармацыйнай сферы з пункту гледжання забеспячэння дзяржавай паўнавартаснай рэалізацыі сваіх суверэнных правоў і інтарэсаў сацыяльна-эканамічнага развіцця.

40. Механізмы дэструктыўнага інфармацыйна-псіхалагічнага ўздзеяння на асобу, грамадства і дзяржаву пастаянна ўдасканальваюцца, а маштабнае маніпуляванне масавай свядомасцю прымае такую ж вастрыню, як барацьба за тэрыторыі, рэсурсы і рынкі. Праз інфармацыйную прастору ажыццяўляецца наўмысная дыскрэдытацыя канстытуцыйных асноў дзяржаў і іх уладных структур, размыванне нацыянальнага менталітэту і самабытнасці, уцягванне людзей у экстрэмісцкую і тэрарыстычную дзейнасць, распальванне міжнацыянальнай і міжканфесійнай варожасці, фарміраванне радыкальнага і пратэснага патэнцыялу. Інфармацыйны фактар адыгрывае ўсё больш значную ролю ў міждзяржаўных канфліктах і няяўных дзеяннях, накіраваных на парушэнне суверэнітэту, тэрытарыяльнай цэласнасці краін і зніжэнне тэмпаў іх развіцця. У выніку інфармацыйных уздзеянняў істотна мяняюцца сацыяльныя сувязі чалавека ў грамадстве, стыль мыслення, спосабы зносін, успрыманне рэчаіснасці і самаацэнка.

Усё большую занепакоенасць выклікае актыўнае распаўсюджванне ў інфармацыйнай прасторы фальсіфікаванай, непраўдзівай і забароненай інфармацыі. Зніжэнне крытычных адносін спажыўцоў інфармацыі да фэйкавых паведамленняў навінавых рэсурсаў, у сацыяльных сетках і на іншых анлайн-платформах стварае перадумовы наўмыснага выкарыстання дэзінфармацыі для дэстабілізацыі грамадскай свядомасці ў палітычных, сацыяльна-небяспечных, іншых падобных мэтах.

41. У сувязі з гэтым асаблівае значэнне набываюць адказныя паводзіны ўсіх удзельнікаў інфармацыйных працэсаў, а таксама выпрацоўка агульных правілаў камунікацыі ў інфармацыйнай прасторы, заснаваных на прызнанні ідэнтычнасці правоў і абавязкаў у існуючай рэальнасці (фізічным свеце) і віртуальнай прасторы.

ГЛАВА 11
Асноўныя кірункі гарантавання бяспекі ў інфармацыйнай прасторы

42. Для Рэспублікі Беларусь асноўнымі крыніцамі пагроз інфармацыйна-псіхалагічнага характару