

Проект

Концепція інформаційної безпеки України

Зміст

Розділ I. Загальні положення

Розділ II. Основи державної політики у сфері інформаційної безпеки

Розділ III. Суб'єкти та механізми забезпечення інформаційної безпеки України

Розділ IV. Здійснення громадського контролю та державно-громадське партнерство в сфері реалізації державної інформаційної політики та забезпечення інформаційної безпеки

Розділ V. Прикінцеві положення

Розділ I. Загальні положення

1. Концепція інформаційної безпеки України (далі – Концепція) покликана закласти основи системного реагування на новітні виклики національній безпеці України в сфері інформаційного простору, що постали перед Українським суспільством і державою.

Агресивна реакція з боку Російської Федерації на реалізацію Українським народом свого стратегічного, геополітичного та цивілізаційного вибору супроводжується збройною агресією та цілеспрямованою деструктивною діяльністю в інформаційному просторі, що має на меті дестабілізувати Українську державу, пропагувати сепаратизм, розпалювати міжнаціональну та міжетнічну ворожнечу і ненависть та руйнувати імідж України на міжнародній арені.

Виклики та загрози національній безпеці України та міжнародній системі безпеки полягають у масштабному використанні Російською Федерацією інформаційного простору, засобів масової інформації та сучасних комунікативних технологій для поширення викривленої та неправдивої інформації з маніпулятивною протиправною метою.

В той же час Концепція покликана затвердити усвідомлення того, що реагування на зазначені виклики та загрози з метою забезпечення безпеки людини і громадянина, Українського суспільства і держави має здійснюватися виключно за умов неухильного дотримання принципів демократичного суспільства та недопущення порушення чи обмеження свободи слова та свободи вираження думки або протиправного втручання держави, органів влади чи інших суб'єктів у діяльність засобів масової інформації.

2. З метою виконання зазначених завдань, Концепція спрямована на створення передумов для розвитку такого потенціалу інформаційної сфери України, за якого забезпечується її випереджальний розвиток, а зовнішні негативні впливи не створюють реальних небезпек національній інформаційній безпеці держави. Ключове завдання системи інформаційної безпеки – забезпечити сталість такого розвитку, не допускаючи негативних впливів з боку сторонніх суб'єктів.

Реалізація на практиці такого підходу до інформаційної безпеки держави може здійснюватися виключно за участі всіх внутрішніх суб'єктів інформаційних відносин та за умов ефективної взаємодії держави з громадянським суспільством, приватним сектором та окремими громадянами в інтересах ефективного розвитку інформаційної сфери і спільного захисту такого розвитку від зовнішніх загроз.

3. Метою Концепції є забезпечення інформаційного суверенітету та визначення підходів до захисту та розвитку національного інформаційного простору для всебічного інформаційного забезпечення українського суспільства.

4. У цій Концепції наведені нижче терміни вживаються у такому значенні:

інформаційна безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також

через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій;

загрози інформаційній безпеці – наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері;

стратегічний контент – це національний інформаційний продукт, який має на меті забезпечити політичну, культурну та духовну цілісність і розвиток української політичної нації;

національний інформаційний продукт – це аудіовізуальний, друкований чи інший продукт, призначений для задоволення інформаційно-комунікативних потреб громадян України, суспільства і держави, створений громадянами або юридичними особами України згідно з чинним законодавством;

державна інформаційна політика – це діяльність держави, спрямована на формування та регулювання середовища, в якому задовольняються інформаційно-комунікативні потреби громадян України, суспільства і держави;

сталий розвиток національного інформаційного простору – такий стан національного інформаційного простору, за якого забезпечується достатній рівень основних потреб та життєво важливих інтересів громадянина, суспільства і держави в інформаційній сфері;

національний інформаційний простір – сукупність всіх інформаційних потоків як національного, так й іноземного походження, які доступні на території держави;

інформаційна сфера – сукупність інформаційних технологій, ресурсів, продукції і послуг, інформаційної інфраструктури, суб'єктів інформаційної діяльності та системи регулювання суспільних інформаційних відносин;

інформаційний суверенітет України – це виключне право України відповідно до Конституції і законодавства України та норм міжнародного права самостійно і незалежно з додержанням балансу інтересів особи, суспільства і держави визначати й здійснювати внутрішні й геополітичні національні інтереси в інформаційній сфері, державну внутрішню й зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір та гарантувати інформаційну безпеку держави;

інформаційна інфраструктура – сукупність організаційних структур і систем, які забезпечують функціонування та розвиток інформаційного простору, засобів інформаційної взаємодії та доступу користувачів до інформаційних ресурсів;

забезпечення інформаційної безпеки – діяльність, спрямована на запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загроз інформаційній безпеці України;

кібернетична безпека (кібербезпека) – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі;

кіберпростір – середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем;

кіберзлочин – суспільно небезпечне винне діяння у кіберпросторі, передбачене чинним законодавством України про кримінальну відповідальність;

кібертероризм – терористична діяльність у кіберпросторі або з його використанням.

Інші терміни вживаються у значенні, визначеному законодавством України.

5. Правову основу інформаційної безпеки становлять Конституція України, Закон України «Про основи національної безпеки України» та інші закони України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Відповідно до цієї Концепції розробляються і затверджуються стратегії, програми та плани якими визначаються цільові настанови, принципи і напрями діяльності суб'єктів забезпечення інформаційної безпеки України.

6. Діяльність державних органів у сфері забезпечення інформаційної безпеки зосереджується на двох напрямках:

- *забезпечення сталого розвитку інформаційного простору України з метою досягнення ним такого рівня, який завдяки своїм властивостям міг би протистояти зовнішнім та внутрішнім загрозам;*
- *забезпечення створення і функціонування системи захисту процесу розвитку інформаційного простору від загроз.*

Інформаційна безпека України забезпечується шляхом захисту національного інформаційного простору від інформаційних загроз та через сприяння його сталому розвитку задля реалізації життєво важливих інтересів та потреб громадянина, суспільства і держави в інформаційній сфері.

7. Основними принципами забезпечення інформаційної безпеки України є:

- верховенство права;
- пріоритетність захисту прав і свобод людини і громадянина в інформаційній сфері;
- своєчасність і адекватність заходів захисту життєво важливих національних інтересів України від реальних і потенційних загроз інформаційній безпеці;
- захист інформаційного суверенітету України;
- свобода думки і слова та вільне вираження своїх поглядів і переконань;
- свобода збирати, зберігати, використовувати та поширювати інформацію;
- захищеність особи від втручання в її особисте та сімейне життя;
- обмеження доступу до інформації виключно на підставі закону;
- гармонізація особистих, суспільних і державних інтересів, відповідальність всього Українського народу за забезпечення інформаційної безпеки;
- розмежування повноважень, взаємодія та відповідальність державних і недержавних суб'єктів забезпечення інформаційної безпеки;
- пріоритетність розвитку та поширення національних інформаційних технологій, ресурсів, продукції та послуг, а також політика постійного поліпшення кількості та технічної якості каналів передачі інформації;
- можливість задіяння в інтересах забезпечення інформаційної безпеки України систем і механізмів міжнародної та колективної безпеки;
- гармонізація інформаційного законодавства з нормами міжнародного права і правовими актами Європейського Союзу.
- захист інформаційного суверенітету, державного суверенітету, конституційного ладу і територіальної цілісності України;
- формування в інформаційному просторі української ідентичності як невід'ємної складової сталого суспільно-політичного дискурсу, а також розвиток культурних потреб національних меншин;
- формування дуальної системи суспільного та комерційного мовлення;

- сприяння розвитку в національному інформаційному просторі контенту, який підтримує збереження і захист загальнолюдських цінностей, інтелектуальний, духовний і культурний розвиток Українського народу.

Розділ II. Основи державної політики у сфері інформаційної безпеки

8. Державна політика у сфері інформаційної безпеки зосереджена на задоволенні та захисті життєво важливих інтересів та потреб громадянина, суспільства і держави в інформаційній сфері щодо:

- продукування, споживання, розповсюдження і розвитку національного стратегічного контенту та інформації в інтересах громадянина, суспільства і держави;
- функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих комп'ютерних систем, що формують інфраструктурну основу внутрішньодержавного інформаційного простору.

9. Основними напрямками державної політики у сфері забезпечення інформаційної безпеки є:

- забезпечення балансу між неухильним дотриманням конституційних прав і свобод людини в інформаційній сфері, зокрема свободи слова, та реалізацією державних функцій щодо своєчасного виявлення, запобігання, припинення та нейтралізації загроз інформаційній безпеці людини і громадянина, суспільства і держави;
- розвиток нормативно-правової бази для регулювання процесів розвитку інформаційного простору і його захисту від зовнішніх загроз та її гармонізація з нормами міжнародного права, вимогами міжнародного співробітництва, нормами і стандартами Європейського Союзу;
- розробка та реалізація ефективної державної інформаційної політики з метою розвитку національного інформаційного простору та гармонізації системи управління і координації між суб'єктами, які реалізують державну інформаційну політику та державну політику в сфері інформаційної безпеки;
- налагодження співпраці держави з громадським та приватним секторами, а також сприяння міжнародному співробітництву з метою реалізації державної інформаційної політики та забезпечення інформаційної безпеки, а також створення якісного національного інформаційного продукту;
- всебічне сприяння, державна підтримка та пріоритетність створення і розповсюдження національного інформаційного продукту, в тому числі за межі України;
- формування дієвої системи стратегічних комунікацій, що базується на підходах розвинутих демократичних держав світу;
- використання українського національного інформаційного продукту для поширення в міжнародному інформаційному середовищі загальнолюдських цінностей та інформаційного розвитку людства, зокрема обмін із закордонними партнерами України баченням, підходами та механізмами протистояння новітнім викликам, спрямованим на демократичні цінності та свободу слова в інформаційному просторі, що були інспіровані деструктивною політикою інших держав.

10. Державна політика у сфері інформаційної безпеки здійснюється з метою недопущення перешкоджання реалізації життєво важливих інтересів і потреб громадянина, суспільства і держави зовнішніми і внутрішніми загрозами національній безпеці в інформаційній сфері, що є запорукою сталого розвитку національного інформаційного простору.

Загрозами національній безпеці України в інформаційній сфері є:

- загрози комунікативного характеру в сфері реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання, розповсюдження та розвитку національного стратегічного контенту та інформації;
- загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору.

11. Загрози комунікативного характеру в сфері реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання, розповсюдження та розвитку національного стратегічного контенту та інформації включають:

- 1) зовнішні негативні інформаційні впливи на свідомість людини та спільноти через засоби масової інформації, а також мережу Інтернет, що здійснюються на шкоду державі та мають на меті:
 - спроби змінювати психічні та емоційні стани людини, її психологічні та фізіологічні характеристики;
 - здійснювати керований вплив на свободу вибору, шляхом поширення у національному інформаційному просторі культу насильства і жорстокості, зневажливого ставлення до людської і національної гідності, розпалювання міжрелігійної, міжетнічної та міжнаціональної ворожнечі, ненависті за етнічною, мовною, релігійною та іншими ознаками;
 - поширення закликів до сепаратизму, повалення конституційного ладу чи порушення територіальної цілісності держави;
- 2) інформаційний вплив на населення України, у тому числі на особовий склад військових формувань, мобілізаційний резерв, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;
- 3) відсутність в державі комплексної системи забезпечення стратегічних комунікацій;
- 4) відсутність загальнонаціональних програм розвитку медіаграмотності, критичного мислення, що може призводити до ефективної реалізації проти громадян деструктивних інформаційних впливів;
- 5) загрози свободі слова, що виражається у:
 - втручанні в редакційну політику з боку власників засобів масової інформації, а також політичних партій та громадських об'єднань;
 - відсутності правової бази для посилення ролі творчих (трудових) колективів і редакцій у процесі здійснення редакційної політики засобами масової інформації усіх форм власності;
 - монопольна концентрація власності на засоби масової інформації та засоби донесення інформації до споживача, що надає можливість здійснювати цілеспрямований вплив на споживачів інформації;

- створення адміністративних і нормативно-правових передумов для обмеження свободи слова, маніпулювання суспільною свідомістю як під зовнішнім впливом, так і з боку внутрішніх політичних організацій, комерційних структур та окремих осіб;
- б) створення, розповсюдження, передача та зберігання інформації з метою підтримки, супроводження чи активізації злочинної та терористичної діяльності.

12. Загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору включають:

- 1) використання іноземними державами кібервійськ, кіберпідрозділів, нових видів інформаційної зброї та зброї кібернетичного характеру на шкоду Україні;
- 2) прояви кіберзлочинності, кібертероризму чи кібернетичної військової агресії, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем, шляхом втручання, несанкціонованого доступу або порушення функціонування телекомунікаційних, кібернетичних, автоматизованих комп'ютерних систем, незалежно від форми власності, з метою:
 - вчинення диверсій чи терористичних актів;
 - здійснення підтримки, супроводження чи активізації злочинної, екстремістської чи терористичної діяльності;
 - здійснення з їх допомогою деструктивного інформаційного впливу;
 - перехоплення інформації в телекомунікаційних мережах;
 - створення радіоелектронних перешкод чи блокування інформаційних систем, засобів зв'язку та управління, реалізація програмно-математичних засобів, що порушують функціонування інформаційних систем;
 - включення у програмно-технічні засоби прихованих шкідливих функцій.
- 3) недостатній рівень розвитку національної інформаційної інфраструктури, зокрема:
 - відсутність національної системи сповіщення про надзвичайні ситуації та інформування населення в таких ситуаціях;
 - низькі темпи впровадження цифрового мовлення та відсутність належного рівня покриття цифровим сигналом території України;
 - залежність національної інформаційної інфраструктури від іноземних виробників високотехнологічної продукції;
 - використання неліцензованого і несертифікованого програмного забезпечення, засобів і комплексів обробки інформації;
 - невідповідність норм юридичної відповідальності за скоєні правопорушення сучасним викликам і загрозам інформаційній безпеці;
 - недостатній рівень захищеності об'єктів критичної інформаційної інфраструктури держави.
- 4) порушення порядку доступу, поводження та встановлених регламентів збору, обробки, зберігання, поширення чи передачі інформації, яка захищається державою (державна таємниця, конфіденційна інформація, персональні дані, авторські права чи інтелектуальна власність), або роботи з інформаційними ресурсами, що її містять;

- 5) відсутність громадського контролю за діяльністю суб'єктів забезпечення інформаційної безпеки, захищеністю національної інформаційної інфраструктури та інформаційного простору України.

13. Державна політика щодо забезпечення інформаційної безпеки на тимчасово окупованих територіях є частиною державної інформаційної політики та полягає у сприянні забезпеченню стабільного функціонування системи національного телебачення і радіомовлення на окупованих територіях, забезпечення громадян на цих територіях об'єктивною та повною інформацією про події в Україні та світі, а також реінтеграція інформаційного простору окупованих територій до загальноукраїнського інформаційного простору.

Держава має забезпечити створення дієвої системи інформаційної присутності України в інформаційному просторі окупованих територій, а також здійснювати системні заходи для підтримки виробників національного інформаційного продукту на окупованих територіях

Розділ III. Суб'єкти та механізми забезпечення інформаційної безпеки України

14. Суб'єктами забезпечення інформаційної безпеки є:

- громадяни України, об'єднання громадян, громадські організації та інші інститути громадянського суспільства;
- Президент України, Верховна Рада України, Кабінет Міністрів України, інші центральні органи виконавчої влади та органи сектору безпеки і оборони України;
- засоби масової інформації та комунікації різних форм власності, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність;
- наукові установи, освітні і навчальні заклади України, які, зокрема, здійснюють наукові дослідження та підготовку фахівців за різними напрямками інформаційної діяльності, в галузі інформаційної безпеки.

15. Центральним органом, спеціально уповноваженим здійснювати координацію та контроль забезпечення інформаційної безпеки як складової національної безпеки і оборони в межах компетенції та покладених на нього функцій, є Рада національної безпеки і оборони України, яка, відповідно до своїх повноважень:

- визначає стратегічні національні інтереси України, концептуальні підходи та напрями забезпечення національної безпеки і оборони в інформаційній сфері;
- формує проекти державних програм, доктрин, законів України, указів Президента України, директив Верховного Головнокомандувача Збройних Сил України, міжнародних договорів, інших нормативних актів і документів з питань інформаційної безпеки України;
- координує і здійснює контроль над іншими державними органами сектору національної безпеки і оборони в сфері забезпечення інформаційної безпеки України;

- здійснює постійний моніторинг впливу на національну безпеку процесів, що відбуваються в інформаційній сфері;
- визначає стан інформаційної агресії та звертається до Верховної Ради України з пропозицією про введення спеціального правового режиму захисту інформаційного простору держави.

16. Основними суб'єктами реалізації державної політики в сфері інформаційної безпеки, в межах їх повноважень та завдань, є:

- Служба безпеки України;
- Міністерство внутрішніх справ України;
- Міністерство оборони України;
- Служба зовнішньої розвідки України;
- Центральний орган виконавчої влади із спеціальним статусом, який забезпечує формування та реалізує державну політику у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій і користування радіочастотним ресурсом України.

17. Формування, реалізацію та координацію державної інформаційної політики, а також забезпечення інформаційного суверенітету України здійснює спеціально уповноважений центральний орган виконавчої влади відповідно до покладених на нього функцій.

Завданнями центрального органу виконавчої влади в сфері державної інформаційної політики є:

- розробка концептуальних документів в сфері сталого розвитку інформаційного простору та контроль за їх виконанням в системі органів виконавчої влади;
- координація діяльності центральних органів виконавчої влади щодо забезпечення сталого розвитку інформаційного простору України;
- участь у формуванні та реалізації стратегій, програм та планів, якими визначаються цільові настанови, принципи і напрями реалізації положень цієї Концепції;
- підготовка нормативних документів, що регламентують порядок зв'язків з громадськістю органів державної влади та оприлюднення інформації про їх діяльність, а також координація та контроль діяльності підрозділів центральних органів виконавчої влади, що здійснюють комунікацію з громадськістю.

18. Основними суб'єктами реалізації державної інформаційної політики України є органи виконавчої влади, які формують та реалізують державну політику в наступних напрямках:

- у сферах освіти і науки, інтелектуальної власності, наукової, науково-технічної та інноваційної діяльності, інформатизації, формування і використання національних електронних інформаційних ресурсів, створення умов для розвитку інформаційного суспільства, а також у сфері здійснення державного нагляду (контролю) за діяльністю навчальних закладів незалежно від їх підпорядкування і форми власності;
- у сферах культури та мистецтв, охорони культурної спадщини, вивезення, ввезення і повернення культурних цінностей, державної мовної політики, а також у сфері формування та реалізації державної політики у сфері кінематографії;

- у сфері інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства;
- у сфері телебачення і радіомовлення, інформаційній та видавничій сферах.
- у сфері зовнішніх зносин України

19. Спеціально уповноважений центральний орган виконавчої влади, що здійснює формування, реалізацію та координацію державної інформаційної політики, а також основні суб'єкти реалізації державної інформаційної політики, здійснюють свою діяльність у взаємодії з:

- постійно діючим колегіальним органом, метою діяльності якого є нагляд за дотриманням законів України у сфері телерадіомовлення, а також здійснення регуляторних повноважень (Національна рада України з питань телебачення і радіомовлення);
- органом державного регулювання у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом та надання послуг поштового зв'язку;
- органами саморегуляції медіасфери України.

20. Ця Концепція, її ключові положення та завдання реалізуються через сукупність нормативно-правових актів, відповідальність за розробку і виконання яких несуть суб'єкти забезпечення сталого інформаційного розвитку та інформаційної безпеки, визначені цією Концепцією.

Спеціально уповноважений центральний орган виконавчої влади в сфері реалізації державної інформаційної політики вживає заходів щодо забезпечення цілісності та узгодженості політики у сфері інформаційної безпеки та захисту інформаційного суверенітету України.

Спеціально уповноважений центральний орган виконавчої влади в сфері реалізації державної інформаційної політики формує та подає на розгляд Кабінету Міністрів України пропозиції щодо розробки, прийняття та виконання нормативно-правових актів, які скеровують та координують інформаційну діяльність Кабінету міністрів України, Прем'єр-міністра України, членів Кабінету міністрів України, міністерств та інших центральних органів виконавчої влади та їхніх посадових осіб, а також Антимонопольного комітету України, Фонду державного майна України та їхніх посадових осіб.

Спеціально уповноважений центральний орган виконавчої влади в сфері реалізації державної інформаційної політики формує та подає на розгляд Ради національної безпеки та оборони України пропозиції щодо розробки, прийняття та виконання нормативно-правових актів, які скеровують та координують інформаційну діяльність Президента України, Ради національної безпеки та оборони України, Міністерства оборони України, вищого командування Збройних Сил України, Міністерства закордонних справ України, Служби безпеки України, Національного антикорупційного бюро України, Державної прикордонної служби України, розвідувальних та контррозвідувальних органів, місцевих державних адміністрацій.

Спеціально уповноважений центральний орган виконавчої влади в сфері реалізації державної інформаційної політики формує та подає на розгляд Національного банку України та Генеральної прокуратури України пропозиції щодо розробки, прийняття та виконання нормативно-правових актів, які регулюють їхню інформаційну діяльність.

Кабінет Міністрів України, Рада національної безпеки та оборони України, Національний банк України, Генеральна прокуратура України розглядають у встановленому порядку пропозиції спеціально уповноваженого центрального органу виконавчої влади в сфері реалізації державної інформаційної політики та приймають відповідні рішення в межах своїх повноважень.

На виконання розпоряджень Кабінету Міністрів України, Ради національної безпеки та оборони України, прийнятих на основі пропозицій центрального органу виконавчої влади в сфері реалізації державної інформаційної політики, органи виконавчої влади, які є суб'єктами реалізації державної інформаційної політики, забезпечують реалізацію положень цієї Концепції.

Спеціально уповноважений центральний орган виконавчої влади в сфері реалізації державної інформаційної політики приймає та розглядає звернення інших державних органів, громадян України, громадських об'єднань і організацій для їх врахування під час розробки пропозицій Кабінету Міністрів України та іншим органам виконавчої влади.

21. Нормативно-правовими актами, які забезпечують реалізацію цієї Концепції, є:

- Державна програма розвитку інформаційного простору України;
- Державна програма забезпечення загальнонаціонального доступу до мережі Інтернет;
- Державна програма підтримки вітчизняного ІТ-виробництва;
- Державна програма з питань іномовлення та представлення України в міжнародному інформаційному просторі;
- Державна програма з питань єдиної офіційної комунікативної політики;
- Державна програма розвитку державно-приватного партнерства в інформаційній сфері;
- Державна програма захисту культурних та інформаційних потреб громадян України, розвитку медіаграмотності/медіаосвіти;
- Державна програма забезпечення кібернетичної безпеки України
- Державна програма підготовки і перепідготовки спеціалістів з інформаційної безпеки;
- Державна програма наукового та моніторингового забезпечення інформаційної сфери.

Розробка та виконання зазначених документів є складовою частиною обов'язків суб'єктів забезпечення сталого інформаційного розвитку та інформаційної безпеки України.

Контроль за дотриманням виконання зазначених документів, їх узгодженості між собою за цілями та заходами в межах конкретних напрямів, покладається на органи, що згідно з положеннями цієї Концепції відповідають за координацію та контроль забезпечення сталого інформаційного розвитку та інформаційної безпеки України.

Державні програми які забезпечують реалізацію Концепції інформаційної безпеки мають реалізуватись на прозорих конкурентних засадах.

Розділ IV. Громадський контроль та державно-громадське партнерство в сфері реалізації державної інформаційної політики та забезпечення інформаційної безпеки

22. Форми громадського контролю у сфері реалізації державної інформаційної політики визначаються нормативно-правовими актами України про діяльність громадських рад та нормами цієї Концепції.

Громадський контроль у сфері забезпечення інформаційної безпеки здійснюється у формах, що визначені Радою національної безпеки та оборони України і не суперечать чинному законодавству України з питань громадського контролю.

23. Основним напрямом здійснення громадського контролю у сфері реалізації державної інформаційної політики є формування спеціальних Експертних рад при спеціально уповноваженому центральному органі виконавчої влади в сфері реалізації державної інформаційної політики. Експертні ради створюються задля здійснення контролю громадськості за процесом формування, виконання та результативності нормативно-правових актів, що вказані в цій Концепції та забезпечують її реалізацію.

Положення про Експертні ради розробляється та затверджується спеціально уповноваженим центральним органом виконавчої влади в сфері реалізації державної інформаційної політики. Склад Експертних рад формується з науковців, освітян, представників органів самоорганізації населення та громадських організацій (за напрямом конкретної державної програми). До складу Експертних рад можуть бути додатково включені (без права голосу) представники державних структур, у тому числі тих, що відповідають за реалізацію конкретних програм. За рішенням керівника спеціально уповноваженого центрального органу виконавчої влади в сфері реалізації державної інформаційної політики голови Експертних рад, що обрані зі складу цих Експертних рад, призначаються радниками керівника спеціально уповноваженого центрального органу на громадських засадах.

Основні завдання профільних Експертних рад з контролю за виконанням нормативно-правових актів, які забезпечують реалізацію цієї Концепції:

- підготовка пропозицій на етапі формування проектів нормативно-правових актів, які забезпечують реалізацію цієї Концепції;
- опрацювання проміжних звітів та незалежна оцінка процесу виконання зазначених програм, що надається суспільству незалежно від оцінки спеціально уповноваженого центрального органу виконавчої влади в сфері реалізації державної інформаційної політики;
- підготовка цільових пропозицій щодо підвищення ефективності реалізації положень програм;
- запрошення на засідання Експертних рад представників структур, що визначені в якості відповідальних за виконання програм;
- формування фінальних звітів щодо ефективності реалізації державних програм.

Розділ VI. Прикінцеві положення

24. Ця Концепція набирає чинності з дня її опублікування. На підставі цієї Концепції внести відповідні зміни до діючих законодавчих актів: Закону України «Про інформацію», Закону України «Про Кабінет Міністрів України» (п.4 Статті 3; п.1 Статті 47) та інших нормативно-правових актів; привести їх у відповідність до цієї Концепції.

Доручити Кабінету Міністрів України привести у відповідність підзаконні нормативно-правові акти та внести на розгляд Верховної Ради України проекти законів про наступні державні програми:

- Державну програму розвитку інформаційного простору України;
- Державну програму доступу до мережі Інтернет;
- Державну програму підтримки вітчизняного ІТ-виробництва;

- Державну програма з питань іномовлення та представлення України в міжнародному інформаційному просторі;
- Державну програма з питань єдиної офіційної комунікативної політики;
- Державну програма розвитку державно-приватного партнерства в інформаційній сфері;
- Державну програма захисту культурних та інформаційних потреб громадян України, розвитку медіаграмотності/медіаосвіти;
- Державну програма забезпечення кібернетичної безпеки України
- Державну програма підготовки і перепідготовки спеціалістів з інформаційної безпеки;
- Державну програма наукового та моніторингового забезпечення інформаційної сфери.