НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут неперервної освіти
Кафедра публічного управління та адміністрування

Галина Нестеренко

ІНФОРМАЦІЙНА БЕЗПЕКА
курс лекцій

КИЇВ-2022

УДК 351:004.056

Схвалено на засіданні кафедри публічного управління та адміністрування,
(протокол № 7 від 08 грудня 2022 року)

Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

Курс лекцій підготовлено відповідно до робочої програми навчальної дисципліни «Інформаційна безпека» та містить основні тексти лекцій, що відповідають визначеній програмою тематиці. Подано теоретичний та аналітичний матеріал щодо основних засад інформаційної безпеки держави; класифікації національних інтересів та загроз інформаційній безпеці; міжнародної та вітчизняної нормативно-правової бази у сфері забезпечення інформаційної безпеки; напрямів державної політики інформаційної безпеки, структури та повноважень органів, що забезпечують інформаційну безпеку та кібербезпеку в Україні; національного інформаційного простору та системи національних інформаційних ресурсів, проблем забезпечення стійкості національного інформаційного простору.

Рекомендовано для здобувачів вищої освіти освітнього ступеня «Бакалавр» усіх форм навчання спеціальності «Публічне управління та адміністрування».

«Розвиток і освіта жодній людині
не можуть бути дані або повідомлені.
Усяк, хто бажає до них долучатися
повинен досягнути цього власною діяльністю, власними
силами, власним напруженням»
(А.Дістервег)

«Хто володіє інформацією – володіє світом»
(Уінстон Черчель)

З М І С Т

ПЕРЕДМОВА

Навчальна дисципліна «Інформаційна безпека» є важливою складовою формування профілю фахівця у галузі публічного управління та адміністрування і належить до циклу дисциплін професійної підготовки здобувачів вищої освіти ступеня бакалавра спеціальності 281 «Публічне управління та адміністрування».

Метою навчальної дисципліни є формування у здобувачів вищої освіти теоретичних знань та практичних навичок щодо забезпечення інформаційної безпеки національних інтересів у будь-якій сфері життєдіяльності суспільства.

Основними завданнями навчальної дисципліни є:

- ✓ формування знань щодо концептуальних засад, принципів, форм та методів забезпечення інформаційної безпеки;
- ✓ ознайомлення з ключовими загрозами інформаційної безпеки, основами управління інформаційною безпекою;
- ✓ вироблення навичок використання знань теорії і практики інформаційної безпеки у практиці публічного управління.

Курс лекцій містить основні тексти лекцій, що відповідають навчальній програмі дисципліни «Інформаційна безпека». Розглянуто теоретичні засади інформаційної безпеки держави, зокрема розглянуто понятійний апарат у сфері інформаційної безпеки та кібербезпеки, з'ясовано сутність та визначено класифікації національних інтересів та загроз інформаційній безпеці. Розглянуто та проаналізовано міжнародну та вітчизняну нормативно-правову базу у сфері забезпечення інформаційної безпеки, з'ясовано напрями державної політики інформаційної безпеки, розглянуто структуру та повноваження органів, що забезпечують інформаційну безпеку та кібербезпеку в Україні. Розглянуто основні поняття національного інформаційного простору та визначено систему національних інформаційних ресурсів, проаналізовано проблеми забезпечення стійкості національного інформаційного простору.

Тема 1. ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИ

Інформаційна безпека: понятійний апарат

Стаття 3 Конституції України визначає, що «Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю.

Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави» [11].

Стаття 17. Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави [11].

Інформація – це відомості про особи, предмети, факти, явища і процеси незалежно від форми їхнього подання.

Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [27].

Інформаційний продукт – це:

документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;

документована інформація, яку підготовлено відповідно до потреб користувачів і яка призначена для задоволення потреб користувачів;

створена виробником сукупність документованої інформації, відомостей, даних і знань, яка призначена для забезпечення інформаційних потреб користувача [8].

Під ***інформаційним середовищем*** розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно поділяється на три основні частини:

створення і розповсюдження вихідної та похідної інформації;

формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;

споживання інформації;

та дві забезпечувальні предметні частини:

створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;

створення і застосування засобів і механізмів інформаційної безпеки.

Інформаційний простір – це:

1) інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, захисту та поширення інформації, інформаційних продуктів і ресурсів, на яке поширюється юрисдикція держави;

2) сукупність національних інформаційних ресурсів та інформаційної інфраструктури, які дозволяють на основі єдиних принципів і загальних правил забезпечувати інформаційну взаємодію громадян, суспільства і держави з їх рівним правом доступу до відкритих інформаційних ресурсів та максимально повним задоволенням інформаційних потреб суб’єктів держави на всій її території з додержанням балансу інтересів на входження у світовий інформаційний простір і забезпечення інформаційної безпеки відповідно до Конституції України та міжнародних правових норм [8].

Інформаційні ресурси:

1) сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо);

2) організована сукупність інформаційних продуктів певного призначення, що необхідні для забезпечення інформаційних потреб громадян, суспільства, держави в певній сфері життя чи діяльності [8].

Інформаційні правовідносини – суспільні відносини, які виникають, змінюються та припиняються у зв'язку з інформацією, яка є їх об'єктом.

Суб'єктами інформаційних відносин є: фізичні особи; юридичні особи; об'єднання громадян; суб'єкти владних повноважень.

Об'єктом інформаційних відносин є інформація.

Інформація, що захищається – це інформація, що є предметом власності якого-небудь суб'єкта (держави, відомства, групи осіб або окремого громадянина) і підлягає захисту відповідно до вимог правових норм або вимог, які встановлюються власником інформації. До такого типу інформації належить інформація з обмеженим доступом і критична інформація.

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [27].

Інформаційна безпека є складовою національної безпеки держави. Особливістю інформаційної безпеки є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, військової, освітньої, політичної безпеки тощо.

Інформаційна безпека України є складовою частиною національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії

нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [35].

Відповідно до закону України «Про інформацію» забезпечення інформаційної безпеки є одним із основних напрямів державної інформаційної політики [27].

Базовою характеристикою інформаційної безпеки слід вважати імовірність появи загрози підвищеного ризику реалізації загрози або небезпеки для індивіда, суспільства та держави. Критерієм ефективності забезпечення інформаційної безпеки є високий рівень безпеки при мінімумі відповідних витрат.

Сукупність внутрішніх і зовнішніх інформаційних загроз створюють передумови для порушення безпечного функціонування системи державного управління.

З точки зору інформаційного права ***інформаційна безпека*** – це одна зі сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особи, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

Таким чином, ***інформаційну безпеку держави*** розуміємо як важливу функцію держави, невід'ємну складову національної безпеки крани, яка включає стан захищеності інформаційного простору; стан захищеності національних інтересів держави в інформаційному середовищі; процес управління загрозами та небезпеками, що забезпечує інформаційний суверенітет держави; захищеність установлених законом правил, за якими відбуваються інформаційні процеси в державі; суспільні відносини, пов'язані

із захистом життєво важливих інтересів людини і громадянина, суспільства, держави від реальних та потенційних загроз в інформаційному просторі.

Головним елементом парадигми інформаційної безпеки виступає інформаційний гуманізм, гарантуючий захищеність об'єктів соціальної природи.

Суть інституту інформаційної безпеки в системі інформаційного права полягає в здійсненні правових, організаційних, технічних заходів, що забезпечують безпеку всіх складових інформаційно-комунікаційного комплексу держави, системи інформаційних ресурсів, інформаційно-комунікаційної інфраструктури, науково-технічного та виробничого комплексу інформаційної індустрії, ринку інформаційної продукції та послуг, системи масової інформаційної освіти, просвіти та підготовки професійних кадрів для інформаційної сфери. окремих організацій та кожної людини [6].

Водночас, під інформаційною безпекою доцільно розуміти сукупність суспільних відносин, що складаються в процесі захисту конституційних прав і свобод від внутрішніх і зовнішніх загроз в інформаційній сфері.

Інтереси особи, суспільства та держави в інформаційній сфері

Інформаційну безпеку держави перш за все будемо розглядати як певну ***систему суспільних відносин***, що виникають з приводу створення умов безпечної життєдіяльності держави, суспільства і особи в інформаційному середовищі. Фактично на суспільний характер інформаційної безпеки вказує Стратегія інформаційної безпеки України, яка зазначає, що проведення Російською Федерацією спеціальних інформаційних операцій спрямовується на ключові демократичні інституції, а спеціальні служби держави-агресора намагаються посилити внутрішні протиріччя в Україні та інших демократичних державах. Застосовані Російською

Федерацією технології гібридної війни проти України, у тому числі моделі і механізми інформаційного втручання, поширюються на інші держави, швидко адаптуючись до локальних контекстів та регуляторних політик [35].

Інформаційна безпека – це сталий стан інформаційного середовища, який забезпечує свою цілісність і захист об'єктів при наявності несприятливих внутрішніх та зовнішніх впливів на основі визначення соціальними суб'єктами своїх цінностей, потреб (життєво важливих інтересів) і цілей розвитку.

Що стосується інтересів особи в інформаційній сфері, то вони полягають в забезпеченні вільного доступу до відкритої інформації, правдивості поданої інформації, щоб інформація не мала на меті негативний інформаційний вплив на особистість, не носила антигуманний, аморальний, екстремістський характер, щоб особиста, конфіденційна інформація громадян була належним чином захищена з використанням норм права, щоб система юридичних норм надійним чином гарантувала права громадян в інформаційній сфері.

Інтереси особи в інформаційній сфері полягають у:

– реалізації конституційних прав людини та громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку;

– захисті інформації, що забезпечує особисту безпеку.

Інтереси суспільства в інформаційній сфері полягають у:

– забезпеченні інтересів особи в цій сфері;

– зміцненні демократії;

– створенні правової соціальної держави;

– досягненні та підтриманні суспільного спокою;

– духовному відновленні держави.

Інтереси держави в інформаційній сфері полягають у створенні умов:

– для гармонійного розвитку державної інформаційної інфраструктури;

– для реалізації конституційних прав і свобод людини та громадянина в галузі одержання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності держави, політичної, економічної та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

Національну безпеку України в інформаційній сфері слід розглядати як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки.

Тому в процесі визначення характеру ризиків інформаційної безпеки слід брати до уваги наступні елементи:

– концептуальне засади політичної безпеки, її принципів, стандартів та правил, погоджених із чинним законодавством й принципами забезпечення безперервності системи інформаційної безпеки особистості, суспільства, комерційних (корпоративних) структур та держави;

– визначення об’єктів та цілей;

– визначення прийнятних з погляду забезпечення інтересів усіх суб’єктів структур встановлення контролю над об’єктами безпеки, а також оцінки ризиків та управління ризиками;

– визначення статусно-функціональних ролей, очікувань та міри відповідальності задіяних суб’єктів включно зі звітністю про події, які несуть потенційні загрози [1].

Інформаційна безпека в якості ключової ***складової національної безпеки*** охоплює напрями:

забезпечення захисту інформаційного простору, що підтримує справедливий розподіл благ і ресурсів;

сприяння процесу переходу до стійкого розвитку світового інформаційного середовища, що формується;

стан захищеності культурного генофонду людства в умовах глобалізації [19].

Об'єкти, суб'єкти та види інформаційної безпеки

Система забезпечення інформаційної безпеки складається з таких елементів, як:

суб'єкти безпеки – державні інститути, організації, служби, окремі особистості, які забезпечують безпеку об'єкта на основі практичних дій при введенні в дію механізму забезпечення безпеки й організації практичних дій;

об'єкт безпеки – те, на що спрямовано дії суб'єкта по забезпеченню його безпеки. Об'єктами безпеки на різних ієрархічних рівнях виступають: економічна система держави, галузь народного господарства, економіка регіону, фірма або підприємство будь-якої організаційно-правової форми як господарюючий суб'єкт, домашнє господарство, особистість;

механізм забезпечення безпеки – теоретичне обґрунтування послідовності подій, що відбуваються, й практичних дій щодо забезпечення безпеки.

Класифікація загроз безпеки

Класифікаційна ознака	**Класифікаційні групи**
За джерелом погрози	1) внутрішні — джерело на території України; 2) зовнішні — джерело розташоване за кордоном держави

За природою виникнення загроз	1) викликані політикою держави; 2) ініційовані іноземними державами; 3) що надходять від кримінальних структур; 4) що надходять від конкурентів або контрагентів
За ймовірністю реалізації	1) реальні — можуть здійснюватися в будь-який момент часу; 2) потенційні — можуть реалізуватися у разі формування певних умов
Стосовно людської діяльності	1) об'єктивні — формуються незалежно від цілеспрямованої діяльності; 2) суб'єктивні — створюються свідомо, наприклад, розвідувальною, підривною й іншою діяльністю, організованою злочинністю
За об'єктом зазіхання	1) на інформацію; 2) на майно; 3) на фінанси; 4) на персонал; 5) на ділове реноме
За можливістю прогнозування	1) що прогнозуються на рівні господарюючого суб'єкта; 2) що не піддаються прогнозу
За наслідками	1) загальні — відбуваються на всій території України або більшості її суб'єктів; 2) локальні — мають вплив на окремі об'єкти
За величиною нанесеного (очікуваного) збитку	1) катастрофічні; 2) значні; 3) що спричиняють труднощі

Інформаційна безпека особи – це стан захищеності психіки та здоров'я людини від деструктивного інформаційного впливу, який призводить до

неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану.

Інформаційна безпека суспільства – можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов'язаних із можливістю вільного одержання, створення й поширення інформації, а також ступінь їхнього захисту від деструктивного інформаційного впливу.

Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть завдати збитків чи зашкодити реалізації інформаційних прав, потреб та інтересів країни та її громадян.

Слід зазначити, що інформаційна безпека особи та суспільства між собою тісно пов'язані.

Інформаційна безпека суспільства та його окремих осіб залежить від рівня:

– інтелектуальності, спеціальної теоретичної й практичної підготовки;

– критичного мислення, морального та духовного вдосконалення;

– гармонійного розвитку особи в суспільстві;

– технічних засобів захисту.

Інформаційна безпека держави – це стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам.

Питання для самоконтролю

Основні підходи до визначення поняття «інформаційна безпека»

Перерахуйте основні ознаки інформаційної безпеки.

Які основні визначення поняття «інформаційна безпека».

Що таке інформаційна безпека держави?

У чому полягають інтереси особи, суспільства та держави в інформаційній сфері?

Назвіть об’єкти, суб’єкти та види інформаційної безпеки.

Що таке інформація?

. Що таке джерело інформації?

Які є носії інформації?

Що розуміють під інформаційними ресурсами?

Тема 2. ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Дестабілізуючі фактори інформаційної безпеки. Інформаційні дії та інформаційні загрози, джерела загроз та їх класифікація

У науці «Публічне управління та адміністрування» поняття інформаційної безпеки найчастіше розглядають в контексті національної безпеки країни. Тому під інформаційною безпекою розуміють стан захищеності життєво важливих інтересів особистості, суспільства й держави, при якому зводиться до мінімуму завдання шкоди через неповноту, невчасність та невірогідність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації».

Відповідно до цього, можна виділити три основні ***напрямки забезпечення інформаційної безпеки***:

– захист інформаційних прав і свобод людини і громадянина;

– захист інформаційних ресурсів, у тому числі й інформації з обмеженим доступом, від неправомірного доступу;

– захист суспільства від некорисної і недоброякісної інформації.

Небезпечні інформаційні дії зазвичай розділяють на два ***види***.

Перший пов’язаний зі втратою цінної інформації, що або знижує ефективність власної діяльності, або підвищує ефективність діяльності супротивника, конкурента. Якщо об’єктом такої дії є свідомість людей, то йдеться про розголошування державних таємниць, вербування агентів, спеціальні заходи й засоби для прослуховування, використання детекторів брехні, медикаментозних, біологічних та хімічних впливів на психіку людини. Безпеку від інформаційної дії цього виду забезпечують органи цензури, військової контррозвідки й інші суб’єкти інформаційної безпеки. Якщо ж джерелом інформації служать технічні системи, то йдеться вже про

технічну розвідку, або шпигунство (прослуховування та перехоплення телефонних розмов, радіограм, сигналів інших систем комунікації), проникнення до комп'ютерних мереж, баз даних.

Другий вид інформаційної дії тісно пов'язаний зі впровадженням негативної інформації, що не лише призводить до небезпечних помилкових рішень, але і змушує шкідливо діяти, що приводить суспільство до катастрофи. Інформаційну безпеку даного виду зобов'язані забезпечувати спеціальні структури інформаційно-технічної боротьби. Вони нейтралізують акції дезінформації, ослаблюють маніпулювання громадською думкою, ліквідовують наслідки комп'ютерних атак. Розвиток і впровадження нових інформаційних технологій у різні сфери життєдіяльності суспільства, як і будь-яких інших науково-технічних досягнень, не лише забезпечують комфортність, але й іноді несуть небезпеку.

Найбільш значні ***групи інформаційно-технічних небезпек***.

Перша група пов'язана з швидким розвитком нового класу зброї – інформаційної, що здатна ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства. У відносно мирних умовах інформаційно-психологічні технології можуть застосовуватися в якості спеціальних механізмів управління кризами і провокації жорстокості на території супротивника.

Друга група інформаційно-технічних небезпек для особи, суспільства й держави – це новий клас соціальних злочинів, що ґрунтуються на застосуванні сучасних інформаційних технологій (махінації з електронними грошима, комп'ютерне хуліганство та ін.). Питання забезпечення інформаційної безпеки як однієї із важливих складових національної безпеки держави особливо гостро постає в контексті появи глобальної комп'ютерної злочинності й кібертероризма.

Третя група інформаційних небезпек – використання нових інформаційних технологій у політичних цілях. Яскравим прикладом є вибори Президента США у 2016 році, коли за допомогою інформаційних технологій розповсюджувалась дезінформація щодо кандидатки від демократичної партії Хіларі Клінтон.

Дестабілізуючими факторами у сфері інформаційної безпеки розуміють такі явища та процеси природного і штучного походження, що породжують інформаційні загрози.

Джерелами дестабілізуючих факторів можуть бути як окремі особи, так і організації та їхні об'єднання. Джерелом дестабілізуючих факторів також може бути природне середовище.

Кожному джерелу властиві певні види дестабілізуючих факторів, які можна представити двома групами: міждержавні дестабілізуючі фактори і внутрішньодержавні дестабілізуючі фактори.

Одним із важливих дестабілізуючих факторів є агресивна політика інших держав або їх коаліції, в яких для формування інформаційних загроз створюються та функціонують спеціальні органи і служби.

Особливу групу джерел дестабілізуючих факторів складають інформаційні системи і засоби, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їх проникнення у свідомість особистості або суспільну свідомість, генератором спонтанних загроз, що виникають внаслідок технічних несправностей та інших причин.

Сукупність джерел разом із властивими їм видами дестабілізуючих факторів формують цілий спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави. До них відносяться: викрадення, знищення, втрата, приховування, спотворення, розголошення, фальсифікація, компрометація корисної (істинної) інформації, а також фабрикування, розповсюдження і впровадження дезінформації.

До внутрішньодержавних дестабілізуючих факторів відносять:

- правовий вакуум у більшості питань забезпечення інформаційної безпеки;
- навмисне або ненавмисне порушення законодавства з питань інформаційної безпеки;
- політичні конфлікти;
- зловмисні дії злочинних елементів або груп;
- відмови, збої, технічні помилки інформаційних систем (засобів);
- природні явища (процеси), що ускладнюють одержання, передачу, прийом і зберігання інформації або руйнують інформаційні системи.

Міждержавні дестабілізуючі фактори – це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії і т. ін.).

Також фактори загроз інформаційній безпеці за видовою ознакою поділяють на політичні, економічні, організаційно-технічні.

Під ***політичними факторами загроз інформаційній безпеці*** розуміють:

- зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;
- інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;
- становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;
- знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;

- порушення інформаційних зв'язків унаслідок утворення на території колишнього СРСР нових держав;
- прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;
- низька загальна правова та інформаційна культура сторін.
- перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур — виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;
- критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;
- розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними ***економічними факторами загроз інформаційній безпеці*** інформації є:

- перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур – виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;
- критичний стан вітчизняних галузей промисловості, які виробляють засоби інформатизації та захисту інформації;
- розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними ***організаційно-технічними факторами загроз*** інформаційній безпеці є***:***

- недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;

- недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;
- широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;
- зростання обсягів інформації, яка передається відкритими каналами зв'язку;
- загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері.

Стратегія інформаційної безпеки дає визначення «***інформаційна загроза*** – це потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні».

Загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особи, суспільства й держави в інформаційній сфері.

Основні загрози інформаційній безпеці можна поділити на три групи:

- загрози впливу неякісної інформації (недостовірної, фальшивої дезінформації) на особу, суспільство, державу;
- загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію й інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);
- загрози інформаційним правам і свободам особи (праву на виробництво, поширення, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову

власність на документовану інформацію; праву на захист честі й гідності тощо).

Аналіз та виявлення загроз інформаційної безпеки країни є важливою функцією її забезпечення. Розробка систем, форм та методів захисту інформації залежить саме від точності та систематичності вивчення потенційних загроз.

Загроза інформаційній безпеці є потенційною можливістю порушення режиму інформаційної безпеки. Навмисна реалізація загрози називається ***атакою на інформаційну систему***. Особи, які навмисно реалізують загрози, є ***зловмисниками***.

Найчастіше загроза є наслідком наявності вразливих місць у захисті інформаційних систем, наприклад, неконтрольований доступ до персональних комп'ютерів або неліцензійне програмне забезпечення.

Історія розвитку та функціонування інформаційного середовища показує, що нові вразливі місця (загрози) з'являються постійно. Відповідно розробка засобів захисту інформаційної безпеки щодо усунення потенційних чи реальних загроз відбувається теж постійно. Як правило, засоби захисту інформації з'являються у відповідь на виникаючі загрози.

Так, наприклад, постійно з'являються виправлення до програмного забезпечення фірми Microsoft, що усувають чергові його вразливі місця. Такий підхід до забезпечення безпеки малоефективний, оскільки завжди існує проміжок часу між моментом виявлення загрози та її усуненням. Саме в цей період зловмисник може завдати непоправної шкоди інформації.

У зв'язку з цим більш прийнятним є інший спосіб захисту інформації – спосіб попереджувального захисту, що полягає в розробці механізмів захисту від можливих, передбачуваних і потенційних загроз.

Деякі загрози не можна вважати наслідком цілеспрямованих дій шкідливого характеру. Існують загрози, викликані випадковими помилками

або техногенними явищами. Знання можливих загроз інформаційній безпеці, а також вразливих місць системи захисту, необхідне для того, щоб вибрати найбільш економічні й ефективні засоби забезпечення інформаційної безпеки.

Виходячи з визначення загроз інформаційної безпеки, можна виділити декілька основних джерел загроз, які можуть стосуватися інтересів особистості, суспільства і держави.

Джерела загроз інформаційній безпеці особистості

Інтереси особистості, які необхідно охороняти в інформаційному суспільстві, полягають насамперед у реальному забезпеченні конституційних прав і свобод людини і громадянина на доступ до відкритої інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, а також у захисту інформації, що забезпечує особисту безпеку, духовний та інтелектуальний розвиток.

Найбільш небезпечним джерелом загроз цим інтересам вважається суттєве розширення можливості маніпулювання свідомістю людини за рахунок формування навкруг неї індивідуального «віртуального інформаційного простору», а також можливість використання технологій впливу на її психічну діяльність.

Важливою особливістю способу життя людини в інформаційному суспільстві є суттєве скорочення «інформаційних» відстаней (часу доступу до необхідної інформації), що веде до появи нових можливостей.

Людство підходить до рубежів, за якими інформаційна інфраструктура стає основним джерелом інформації для людини, здійснює безпосередній вплив на її психічну діяльність, на формування її соціальної поведінки.

Проблема формування розумових потреб і мотивації соціальної поведінки поки не має загального вирішення навіть для індустріального

суспільства і ще більше ускладнюється стосовно інформаційного суспільства. Вона є однією з найбільш складних у сучасній психологічній науці.

У цілому структура споживчо-мотиваційної сфери особистості утворюється базовими потребами (згадайте піраміду Маслоу) та похідними потребами, що формуються діючою системою виховання. Способи і форми задоволення цих потреб у значній мірі залежать від інформації і знань, що ми отримуємо з навколишнього світу, зокрема надходять через інформаційну інфраструктуру. Спрямованість використання отриманої інформації визначаються перш за все особистістю та її духовним потенціалом.

Складність процедур, що реалізуються в сучасних технологіях доступу до інформаційних ресурсів, критично збільшують залежність окремої людини від інших людей, які здійснюють розробку інформаційних технологій, визначення алгоритмів пошуку необхідної інформації, її попередньої обробки, приведення до виду, зручного для сприйняття, доведення до споживача. По суті, ці люди формують для людини інформаційний фон його життя, визначають умови, в яких він живе і діє, вирішує свої життєві проблеми. Саме тому вважається виключно важливим забезпечити безпеку взаємодії людини з інформаційною структурою.

Іншим небезпечним джерелом загроз інтересам особистості є використання на шкоду її інтересам персональних даних, що нагромаджуються різноманітними структурами, в тому числі органами державної влади, а також розширення можливості прихованого збирання інформації, що складає його особисту, сімейну таємницю, відомості про її приватне життя.

У першу чергу це зумовлено труднощами реалізації механізмів охорони відомостей (даних), подальшими досягненнями у мікромініатюризації засобів прихованого збирання і передавання інформації.

Джерела загроз інформаційній безпеці суспільства

Інтереси суспільства полягають у захисті життєво важливих інтересів кожного громадянина, забезпечення реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення демократії, досягнення і підтримування суспільної злагоди, підвищення творчої активності населення.

Одним із джерел загроз інтересам суспільства в інформаційній сфері є безперервне ускладнення інформаційних систем і мереж зв'язку критично важливих інфраструктур забезпечення життя суспільства.

Ці загрози можуть проявлятися у вигляді як навмисних, так і ненавмисних помилок, збоїв і відмов техніки, програмного забезпечення, шкідливого впливу зі сторони злочинних структур і кримінальних елементів. Об'єктами реалізації загроз можуть виступати системи енергетичної, транспортної, трубопровідної і деяких інших інфраструктур.

Небезпечним джерелом загроз виступає можливість концентрації засобів масової інформації (ЗМІ)у руках невеликої групи власників.

Ці загрози можуть проявлятися у вигляді маніпуляції суспільною думкою по відношенню до тих чи інших суспільно значимих подій, а також руйнування моральних устоїв суспільства шляхом нав'язування чужорідних цінностей.

Також небезпечним джерелом загроз інформаційної безпеки є розширення масштабів комп'ютерної злочинності.

Ці загрози можуть проявлятися у вигляді спроб здійснення шахрайських операції з використанням глобальних або вітчизняних інформаційно-телекомунікаційних систем, відмивання фінансових коштів, одержаних протиправним шляхом, одержання неправомірного доступу до фінансової, банківської та іншої інформації, яка може бути використаною з корисливою метою.

Джерела загроз інформаційній безпеці держави

Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, встановлення політичної і соціальної стабільності, економічного процвітання, безумовного виконання законів і підтримки міжнародного співробітництва на основі партнерства.

У першу чергу загрози інтересам держави також можуть проявлятися у вигляді отримання протиправного доступу до відомостей, що складають державну таємницю, до іншої конфіденційної інформації, розкриття якої може нанести збитки державі.

Проте найбільш небезпечними джерелами загроз інтересам держави в інформаційному суспільстві може стати неконтрольоване розповсюдження інформаційної зброї та розгортання гонки озброєнь у цій галузі, спроби реалізації концепції ведення інформаційних війн.

Поняття інформаційної зброї визначається як сукупність засобів, методів і технологій, що забезпечують можливість силового впливу на інформаційну сферу протилежної сторони з метою руйнування її інформаційної інфраструктури, системи управління державою, зниження духовного потенціалу суспільства.

Серед найбільш серйозних завдань, які можуть вирішуватися за допомогою сучасної інформаційної зброї, можна виділити наступні:

- створення атмосфери бездуховності та аморальності, негативного відношення до культурної спадщини противника;
- маніпулювання суспільною свідомістю та політичною орієнтацією соціальних груп населення держави з метою створення політичної напруги та хаосу;

- дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою провокації конфліктів, розпалювання недовіри, загострення політичної боротьби, провокування репресій проти опозиції, провокація взаємного знищення;
- зниження інформаційного забезпечення влади та управління, інспірація помилкових управлінських рішень;
- дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;
- провокування соціальних, політичних, національних і релігійних сутичок;
- ініціювання страйків, масових заворушень та інших акцій економічного протесту;
- ускладнення прийняття органами важливих рішень;
- підрив міжнародного авторитету держави, її співробітництва з іншими країнами;
- нанесення втрат життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах.

Руйнівний вплив інформаційної зброї в інформаційному суспільстві може бути більш потужним та ефективним, ніж це уявляється зараз. Це є особливо небезпечним в умовах існування майже монопольного положення компаній невеликої кількості країн на ринку інформаційних продуктів, оскільки це здатне спровокувати бажання використати наявну перевагу для досягнення тієї чи іншої політичної мети.

Класифікація загроз інформаційної безпеки представлена у таблиці 1[1]

[1] Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (29), 2015 р. С.56-61. URL : https://core.ac.uk/download/pdf/47240087.pdf

Таблиця 1 – Класифікація загроз

Критерії загрози	Вид загрози
За видом властивості інформації, що порушується	загрози конфіденційності (витік, перехват, зняття, копіювання, викрадання, розголошення); загрози цілісності (втрата, знищення, модифікація); загрози доступності (блокування);
За характером порушення	порушення конфіденційності даних; порушення працездатності серверів, мережевого обладнання, робочих станцій; незаконне втручання у функціонування серверів, мережевого обладнання, робочих станцій, тощо;
За тяжкістю порушення	незначні помилки; дрібне хуліганство; серйозний злочин / природні і техногенні катастрофи;
За передбаченням наслідків порушника	умисне порушення; ненавмисне порушення;
За мотивацією	зловмисне порушення; незловмисне порушення;

За закінченістю	закінчені; незакінчені;	
За об'єктом дії	загрози, націлені на всю інформаційну систему; загрози, націлені на окремі компоненти СУ КСІІ;	
За причиною виникнення	загрози, які виникли через недостачу засобів технічного захисту; загрози, які виникли через недостачу організаційних заходів;	
За походженням	антропогенні; техногенні; природні;	
За розміром нанесеної шкоди	незначні; значні; критичні;	
За типовими об'єктами інформатизації	загрози безпеці інформації для СУ на базі автономної ЕОМ (без підключення до обчислювальної мережі); загрози безпеці інформації для СУ на базі локальної обчислювальної мережі (без підключення до розподіленої обчислювальної мережі); загрози безпеці інформації для СУ, підключеної до розподіленої обчислювальної мережі;	
За способом реалізації загроз безпеці інформації	1) загрози спеціальної дії на інформацію: механічної; хімічної; акустичної; біологічної; радіаційної; термічної; електромагнітної (електричні імпульси, електромагнітні випромінювання, магнітне поле);	
	2) загрози НСД в СУ КСІІ	
	3) загрози витоку інформації технічними каналами:	
	по радіоканалу; по електричному каналу; по оптичному каналу; по змішаним (параметричним) каналам;	загрози витоку по каналам ПЕМВН;

Ієрархічна класифікація загроз інформаційній безпеці

Глобальні фактори загроз інформаційній безпеці:

- недружня політика іноземних держав у галузі глобального інформаційного моніторингу, розповсюдження інформації, розповсюдження інформації та нових інформаційних технологій;
- діяльність іноземних розвідувальних та спеціальних служб;
- діяльність іноземних політичних та економічних структуру, спрямована проти інтересів держави;
- злочинні дії міжнародних груп, формувань та окремих осіб.

Регіональні фактори загроз інформаційній безпеці:

- використання інформаційної інфраструктури колишнього СРСР для передавання конфіденційної інформації;
- невідповідність інформаційного забезпечення державних та суспільних інститутів сучасним вимогам управління економічними, політичними та соціальними процесами;
- відставання від розвинених країн світу з темпів та масштабів розробки та впровадження нових інформаційних технологій;
- недопустимо високий рівень технологічної залежності держави від зарубіжних держав у зв'язку з широким використанням імпортних засобів обчислювальної техніки, систем телекомунікації, зв'язку та інформаційних технологій;
- розвиток зарубіжних технічних засобів розвідки, та промислового шпигунства, що дозволяє одержати несанкціонований доступ до конфіденційної інформації, у тому числі такої що складає державну таємницю;
- зростання злочинності в інформаційній сфері;

- використання старих методів та засобів захисту національних інформаційних мереж, широке розповсюдження комп'ютерних вірусів, призначених для ураження систем управління та зв'язку;
- відсутність ефективної системи забезпечення цілісності, незмінності та схоронності нетаємної інформації, у тому числі такої, що є інтелектуальною власністю.

Локальні фактори загроз інформаційній безпеці:

- перехоплення електронних випромінювань;
- застосування підслуховуючих пристроїв або закладок;
- дистанційне фотографування;
- розкрадання носіїв інформації та промислових відходів;
- копіювання носіїв інформації з подоланням заходів захисту;
- незаконне приєднання до апаратури та ліній зв'язку;
- упровадження та використання комп'ютерних вірусів і т. ін.

Відтак система загроз інформаційній безпеці має комплексний характер і в загальному вигляді включає в себе загрози безпеці інформації та інформаційної інфраструктури; загрози безпеці суб’єктів інформаційної сфери й соціальних зв’язків між ними від інформаційних впливів; загрози належному порядку реалізації прав та інтересів суб’єктів інформаційної сфери.

До істотних властивостей загроз інформаційній безпеці держави при цьому належать вибірковість, передбачуваність і шкідливість. Зважаючи на динамічність суспільно-політичної обстановки та появу якісно нових небезпечних для нашої держави факторів, закріплення фіксованого переліку загроз інформаційній безпеці України, який до того ж не має вичерпного характеру, є недоцільним. Тобто будь які переліки загроз не є вичерпними і сталими. Джерелами загроз при цьому можуть бути людина, технічні

пристрої, моделі, алгоритми, програми; технологічні схеми обробки; зовнішнє середовище тощо.

Інформаційна безпека є складним, системним, багаторівневим явищем, на стан якого впливають зовнішні і внутрішні чинники, зокрема політична обстановка у світі; внутрішньополітична обстановка в державі; стан і рівень інформаційно-комунікаційного розвитку країни тощо.

Загрози інформаційній безпеці здебільшого супроводжують виникнення й реалізацію загроз в економічний і політичній сферах, у сфері виконання функцій держави тощо, і заподіяння шкоди в інформаційні сфері є передусім засобом досягнення інших цілей.

Поряд із суто корисливою метою в сучасних умовах інформаційні загрози пов'язані з розпалюванням міжнаціональної, міжконфесійної та іншої ворожнечі, дискредитацією правоохоронної системи й органів державної влади загалом, заподіянням шкоди честі, гідності та ділової репутації фізичних осіб, у тому числі публічних, формуванням «образу ворога», «зомбуванням» населення задля створення умов щодо управління масовою свідомістю. При цьому потенціал інформаційної сфери через її інтегрувальний характер і здатність «проникнення» до інших сфер життєдіяльності суспільства внаслідок їх інформаційного обслуговування поки що недостатньо усвідомлюється політиками та правоохоронцями (за винятком виявів кіберзлочинності), однак успішно використовується представниками організованих злочинних співтовариств і політичними супротивниками нашої держави.

Стратегічне інформаційне протистояння нині становить небезпечний компонент гібридної війни, розгорнутої Росією проти України, причому головною загрозою інформаційній безпеці нашої держави сьогодні залишається загроза впливу ворога на інформаційну інфраструктуру, інформаційні ресурси, на суспільство, свідомість і підсвідомість особистості

з метою нав’язати власну систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності

Питання для самоконтролю

Які напрямки забезпечення інформаційної безпеки?

Які інформаційні дії є небезпечними?

Назвіть групи інформаційно-технічних небезпек.

Що таке дестабілізуючі фактори у сфері інформаційної безпеки, наведіть приклади

Визначте політичні фактори загроз.

Визначте економічні фактори загроз.

Визначте організаційно-технічні фактори загроз.

Назвіть джерела загроз інформаційної безпеки особи.

Назвіть джерела загроз інформаційної безпеки суспільства.

Назвіть джерела загроз інформаційної безпеки держави.

Тема 3. СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ. ДЕРЖАВНА ПОЛІТИКА В ІНФОРМАЦІЙНІЙ СФЕРІ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Складовими системи забезпечення інформаційної безпеки держави є:

- нормативно-правова база;
- інституційне забезпечення (структура і завдання органів державної влади у сфері інформаційної безпеки);
- державна політика інформаційної безпеки як інструмент забезпечення інформаційної безпеки;
- ресурсне забезпечення (організаційне, інформаційно-аналітичне, програмно-технічне і режимне, фінансове, матеріально-технічне, кадрове тощо).

Нормативно-правова база забезпечення інформаційної безпеки України

Найвищим рівнем нормативно-правового забезпечення інформаційної безпеки є міжнародні документи, серед яких документи Організації Об'єднаних Націй, її профільних установ, фондів, програм, зокрема, ООН з питань освіти, науки і культури (ЮНЕСКО), Програми розвитку ООН (ПРООН), Міжнародного Союзу Електрозв'язку (МСЕ, International Telecommunication Union, ITU), Всесвітньої організації інтелектуальної власності (ВОІВ) та інших.

Розглядаючи нормативний доробок ООН, насамперед варто згадати такі ключові документи як Декларація прав людини 1948 року, в якій право на вираження своєї думки визнане однією з основних демократичних цінностей, та Міжнародний Пакт про громадянські та політичні права 1966 року. За підсумками діяльності Генеральної Асамблеї ООН прийнято низку

резолюцій з питань розвитку інформаційного суспільства та інформаційної безпеки, серед яких «Необхідність встановлення нового, більш справедливого та більш ефективного міжнародного порядку в галузі інформації та зв'язку» (1978 р.), «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» (починаючи з 1998 року майже щорічно), «Використання інформаційно-комунікаційних технологій в цілях розвитку» (2002 р.), «Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур», (2002, 2003, 2009 р.р.), «Боротьба зі злочинним використанням інформаційної технології» (2002 р.) та багато інших.

Окрему увагу варто звернути на підсумкові документи міжнародних форумів, зокрема Окінавську хартію глобального інформаційного суспільства 2000 року, Декларацію принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті» і План дій, прийнятих на Всесвітньому саміті з інформаційного суспільства (ВСІС, World Summit on Information Society, WSIS) 2003 року.

У Додатку до Програми для інформаційного суспільства, що була прийнята за результатами другого етапу ВСІС у 2005 році, передбачаються основні напрями використання ІКТ як інструмента інформаційного суспільства, за які відповідають міжнародні організації і програми в системі ООН:

– електронний уряд (ПРООН / МСЕ);

– електронний бізнес (Всесвітня торгівельна організація (ВТО) / Конференція ООН з торгівлі і розвитку (ЮНКТАД) / МСЕ / Всесвітній поштовий союз (ВПС);

– електронне навчання (ЮНЕСКО / МСЕ / ООН з промислового розвитку (ЮНІДО);

– електронна охорона здоров'я (Всесвітня організація охорони здоров'я (ВООЗ / МСЕ);

– електронна зайнятість (Міжнародна організація праці (МОП), МСЕ);

– електронна охорона довкілля (ВООЗ / Всесвітня метеорологічна організація (ВМО) / Програма ООН з навколишнього середовища (ЮНЕП) /Програма ООН з населених пунктів (ООН – Габітат) / МСЕ / Міжнародна організація цивільної авіації (ІКАО)

Значну роботу у сфері розвитку інформаційного суспільства та інформаційної безпеки за напрямами своєї діяльності здійснює ЮНЕСКО, яка розробила Декларацію про основні принципи, що стосуються вкладу ЗМІ у зміцнення миру та міжнародного взаєморозуміння, у розвиток прав людини і у боротьбу проти расизму і апартеїду та підбурення до війни (1978 р.), програму «Інформаційне суспільство для всіх» (1996 р.), Загальну декларацію ЮНЕСКО про культурне різноманіття (2001 р.), Рекомендацію про розвиток та використання багатомовності та загальний доступ до кіберпростору (2003 р.), Хартію про збереження цифрового надбання (2003 р.) та інші.

Особливою є роль у міжнародній нормотворчій діяльності Міжнародного союзу електрозв'язку, який бере участь у розробці міжнародних стандартів у сфері ІТ та інформаційної безпеки, формує стратегічні документи з цих питань, зокрема у 2007 році представив Глобальну програму кібербезпеки, яка визначила цілі, принципи і стратегії розробки моделей законодавства в сфері боротьби з комп'ютерною злочинністю, прийняв низку резолюцій, спрямованих на зміцнення довіри та безпеки при використанні інформаційно-комунікаційних технологій і боротьбі із комп'ютерними злочинами.

Активна нормативно-правова діяльність провадиться на європейському рівні, зокрема Рада Європи прийняла Конвенцію про кіберзлочинність

(2001р.), яка набула загальносвітового значення і була підписана близько 50 країнами світу, Конвенцію про захист осіб стосовно автоматизованої обробки персональних даних (1981 р.), низку резолюцій та рекомендацій Кабінету міністрів з ключових питань розвитку інформаційного суспільства тощо.

Міжнародні стандарти у сфері інформаційної безпеки представлені багатьма стандартами, серед яких насамперед варто згадати такі: ISO/IEC 27000 - серія міжнародних стандартів, яка містить стандарти з інформаційної безпеки, опубліковані спільно Міжнародною організації зі стандартизації (ISO) і Міжнародною електротехнічною комісією (IEC). Серія включає кращі практики і рекомендації в галузі інформаційної безпеки для створення, розвитку і підтримання системи менеджменту інформаційної безпеки; CoBiT (англ. Control Objectives for Information and Related Technology («Завдання інформаційних і суміжних технологій») - відкритий IT-стандарт, який в свою чергу містить ряд документів зі стандартами щодо оптимізації управління IT: аудитом IT та IT-безпекою.

На думку фахівців, ***нормативно-правова база інформаційної безпеки*** має виконувати в першу чергу три ***основні функції***:

– регулювати взаємовідносини між суб'єктами інформаційної безпеки, визначати їх права, обов'язки та відповідальність;

– нормативно забезпечувати дії суб'єктів інформаційної безпеки на всіх рівнях, а саме - людини, суспільства, держави;

– встановлювати порядок застосування різних сил і засобів забезпечення інформаційної безпеки.

За роки незалежності в Україні закладено законодавчі основи системи забезпечення інформаційної безпеки, зокрема було напрацьовано великий масив нормативно-правових актів.

Розглянемо структуру вітчизняного законодавства у сфері інформаційної безпеки. На вершині «піраміди» знаходиться основний закон –

Конституція України, прийнята 28 червня 1996 року, яка закладає основи системи забезпечення інформаційної безпеки. Конституція встановлює, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави, гарантує кожному громадянину права в інформаційній сфері: свободу думки й слова, свободу вираження поглядів і переконань, право вільно збирати, зберігати, використовувати й поширювати інформацію, захист інтелектуальної власності, їхніх авторських прав тощо.

Законодавчі акти Верховної Ради України, розпорядчі документи Президента та Кабінету Міністрів України з питань інформаційної безпеки України, які становлять каркас нормативно-правової бази, за сферою регулювання можна поділити на такі тематичні групи:

1) концептуальні засади інформаційної безпеки як складової національної безпеки

– Закон України «Про національну безпеку України» (2018)

– Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» (2015)

– Указ Президента України від 15 березня 2016 року №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» (2016)

– Указ Президента «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» (2021).

2) використання, розповсюдження інформації

– Закон України «Про інформацію» (1992);

– Закон України «Про друковані засоби масової інформації (пресу) в Україні» (1992);

– Закон України «Про телебачення і радіомовлення» (1993);

– Закон України «Про доступ до публічної інформації» (2011);

– Закон України «Про Суспільне телебачення і радіомовлення України» (2014).

3) використання інформації з обмеженим доступом

– Закон України «Про державну таємницю» (1994);

– Постанова Кабінету Міністрів України від 19 жовтня 2016 р. № 736 «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» (2016);

– Закон України «Про Національну систему конфіденційного зв'язку» (2002);

– Закон України «Про захист персональних даних» (2010).

4) розвиток інформаційного суспільства, інформатизація

– Закон України «Про Національну програму інформатизації» (1998)

– Закон України «Про Концепцію Національної програми інформатизації» (1998)

– Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» (2007)

– Розпорядження Кабінету Міністрів України від 15.05.2013 № 386-р «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» (2013)

– Розпорядження Кабінету Міністрів України від 08.11.2017 №797-р «Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації».

5) зв'язок, ІКС, технічний захист інформації

– Закон України «Про захист інформації в інформаційно-комунікаційних системах» (1994)

– Закон України «Про зв'язок» (1995)

– Закон України «Про державну підтримку розвитку індустрії програмної продукції» (2012)

– Закон України «Про електронні комунікації» (2020)

– Постанова Кабінету Міністрів України від 08.10.1997 № 1126 «Про затвердження Концепції технічного захисту інформації в Україні» (1997)

6) електронні системи інформації

– Закон України «Про електронні документи та електронний документообіг» (2003)

– Закон України «Про електронні довірчі послуги» (2017)

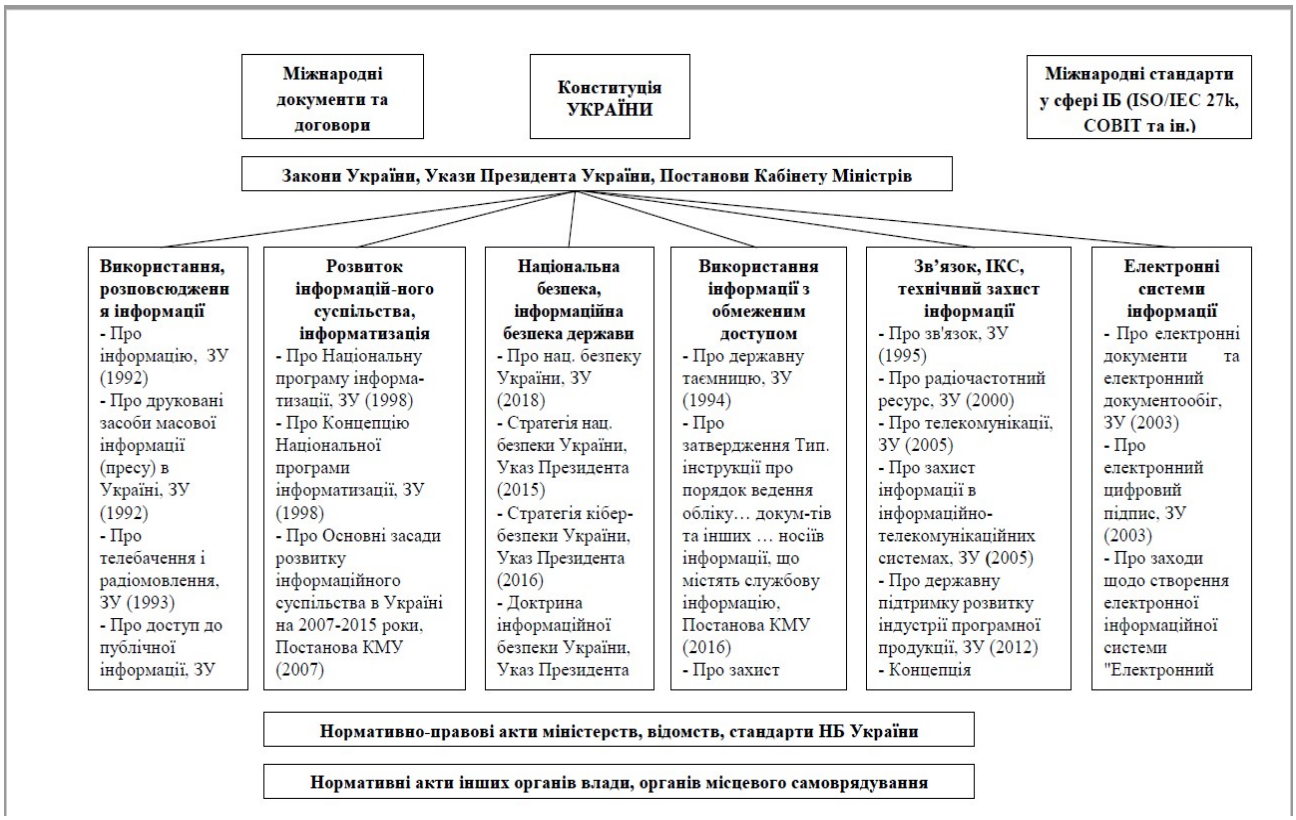
– Постанова Кабінету Міністрів України від 24.02.2003 № 208 «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд» (2003)

– Розпорядження Кабінету Міністрів України від 16.11.2016 № 918-р «Про схвалення Концепції розвитку системи електронних послуг в Україні»

– Розпорядження Кабінету Міністрів України від 20.09.2017 № 649-р «Про схвалення Концепції розвитку електронного урядування в Україні»

Нормативні акти міністерств, відомств, Національного банку України, інших органів влади, органів місцевого самоврядування регулюють питання інформаційної безпеки у межах своєї компетенції.

Загальна схема нормативно-правового забезпечення інформаційної безпеки в Україні представлена на рис. 1.



Інституційне забезпечення інформаційної безпеки України

В Україні сформована та діє достатньо розгалужена система органів державної влади, які виконують функції із забезпечення інформаційної безпеки у різних аспектах.

Систему суб'єктів забезпечення інформаційної безпеки можна визначити як організовану державою сукупність суб'єктів – органів законодавчої, виконавчої, судової влади, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів в інформаційній сфері, що здійснюють узгоджену діяльність у межах законодавства України.

Характеризуючи систему інституційного забезпечення інформаційної безпеки України, слід відзначити, що до її складу входять:

- законодавчий орган – Верховна Рада України, в якій питаннями інформаційної безпеки займаються два комітети: Комітет з питань гуманітарної та інформаційної політики, Комітет з питань свободи слова, Комітет з питань цифрової трансформації. На Уповноваженого Верховної Ради України з прав людини покладено обов'язки щодо захисту персональних даних;
- Президент України як глава держави і Верховний головнокомандувач, координуючу функцію у сфері інформаційної безпеки виконує Рада національної безпеки та оборони (РНБО) України;
- Кабінет Міністрів України як вищий орган у системі органів виконавчої влади;
- два регуляторних органи виконавчої влади – Національна рада України з питань телебачення і радіомовлення та Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку;
- органи виконавчої влади - Державний комітет телебачення та радіомовлення України, Міністерство культури та інформаційної політики України, Міністерство цифрової трансформації України, Державна служба спеціального зв'язку та захисту інформації України, а також міністерства та відомства т.зв. «силового» напряму (Служба безпеки України, Міністерство внутрішніх справ України, Міністерство оборони України та Служба зовнішньої розвідки України). Окрім того, виконання тих чи інших завдань та програм в інформаційній сфері здійснюють понад 20 інших органів державної влади України: Міністерство юстиції України, Міністерство закордонних справ України, Міністерство освіти і науки України, Міністерство інфраструктури України, Державна архівна служба України, інші;
- місцеві органи виконавчої влади, органи місцевого самоврядування;

- органи судочинства (місцеві, апеляційні, спеціалізовані суди, Верховний Суд України);
- організації громадянського суспільства, громадяни.

Єдиним органом законодавчої влади в Україні є парламент – *Верховна Рада України*. До повноважень ВР України належать, зокрема: прийняття законів, визначення засад внутрішньої і зовнішньої політики держави, затвердження загальнодержавних програм, надання законом згоди на обов'язковість міжнародних договорів України та денонсація міжнародних договорів України, здійснення парламентського контролю тощо.

Верховна Рада України для здійснення законопроектної роботи, підготовки і попереднього розгляду питань у межах її повноважень, виконання контрольних функцій створює з числа народних депутатів України комітети Верховної Ради України.

Законодавчою діяльністю з питань інформаційної безпеки опікуються такі комітети Верховної Ради України:

Комітет з питань гуманітарної та інформаційної політики

Основний напрям діяльності Комітету це розробка та вдосконалення законодавчої бази України, що регулює суспільні відносини у гуманітарній та інформаційній сферах. Напрямами діяльності Комітету в інформаційній сфері є:

– медійна індустрія (телебачення, OTT та IPTV, платформи з розповсюдження інформації, радіо), національна кіноіндустрія;

– аудіовізуальний ринок;

– друковані, електронні засоби масової інформації, у тому числі соціальні медіа, мережа Інтернет;

– державна політика у сфері інформації та інформаційної безпеки (крім питань, що належать до сфери національної безпеки та оборони);

У своїй діяльності Комітет співпрацює з центральними органами державної влади, які опікуються питаннями інформаційної та гуманітарної політики, проводить парламентські заходи з громадськістю.

Комітет з питань свободи слова:

Сфера повноважень Комітету включає нормотворчу діяльність у сфері інформаційної політики за такими напрямами:

– забезпечення свободи слова;

– права громадян на інформацію;

– захист прав та свобод працівників ЗМІ;

– гарантії діяльності засобів масової інформації, захист прав журналістів і працівників засобів масової інформації.

Комітет з питань цифрової трансформації

Основний напрям діяльності Комітету – розробка, вдосконалення законодавчої бази України з питань цифрової трансформації, електронної демократії, а саме:

– законодавчі засади цифровізації та цифрового суспільства в Україні;

– Національна та державні програми інформатизації;

– програми ЄС «Єдиний цифровий ринок» (Digital Single Market, EU4Digital) та інші програми цифрового співробітництва;

– інновації у сфері цифрового підприємництва;

– дослідницькі центри у сфері цифрових технологій;

– цифрова індустрія та телекомунікації;

– електронне урядування та публічні електронні послуги;

– електронна демократія;

– електронні довірчі послуги та цифрова ідентифікація;

– державні інформаційно-аналітичні системи, електронний документообіг;

– державні інформаційні ресурси, електронні реєстри та бази даних;

– електронна комерція (електронна торгівля, електронний бізнес);

– розвиток сфери "відкритих даних";

– радіочастотний ресурс;

– розвиток орбітальної економіки;

– законодавчі засади адміністрування, функціонування та використання мережі Інтернет в Україні;

– кібербезпека та кіберзахист, у тому числі у сфері критичної інфраструктури;

– технічний та криптографічний захист інформації;

– розвиток цифрових компетентностей, цифрові права.

Повноваження щодо контролю за додержанням законодавства про захист персональних даних покладено на *Уповноваженого Верховної Ради України з прав людини*.

Згідно зі статтею 23 Закону України «Про захист персональних даних» у сфері захисту персональних даних Уповноважений має такі повноваження:

– отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду;

– проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних;

– отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних;

– затверджувати нормативно-правові акти у сфері захисту персональних даних у випадках, передбачених законодавством;

– за підсумками перевірки, розгляду звернення видавати обов’язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних;

– надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз’яснювати права і обов'язки відповідних осіб за зверненням суб’єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб;

– взаємодіяти із структурними підрозділами або відповідальними особами, які організовують роботу, пов’язану із захистом персональних даних при їх обробці;

– складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом;

– інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов’язки суб’єктів відносин, пов’язаних із персональними даними;

– здійснювати моніторинг нових практик, тенденцій та технологій захисту персональних даних;

– організовувати та забезпечувати взаємодію з іноземними суб’єктами відносин, брати участь у роботі міжнародних організацій з питань захисту персональних даних.

З метою забезпечення виконання Уповноваженим функцій контролю за виконанням законодавства в сфері захисту персональних даних в Секретаріаті Уповноваженого Верховної Ради України з прав людини створено Департамент з питань захисту персональних даних.

Президент України є главою держави, гарантом державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина.

Президент спільно з Верховною Радою визначає державну інформаційну політику, а також політику у галузі захисту інформації, державну політику на телебаченні та радіомовленні, законодавчі основи її реалізації, гарантування соціальної та правового захисту співробітників інформаційної сфери.

Крім того, Президент України:

– керує в межах своїх конституційних повноважень органами і силами з забезпечення інформаційної безпеки;

– санкціонує заходи, щодо забезпечення інформаційної безпеки;

– формує, реорганізує та ліквідує органи і сили з забезпечення інформаційної безпеки.

Координуючу функцію у сфері інформаційної безпеки виконує *Рада національної безпеки та оборони України (РНБО)*. Президент України у своїй діяльності спирається на апарат Ради національної безпеки та оборони.

Рада національної безпеки і оборони України подає пропозиції Президентові України щодо:

– визначення стратегічних національних інтересів України, концептуальних підходів та напрямів забезпечення інформаційної безпеки, заходів політичного, економічного, соціального, воєнного, науково-технологічного, екологічного, інформаційного та іншого характеру відповідно до масштабу потенційних та реальних загроз національним інтересам України;

– забезпечення і контролю надходження та опрацювання необхідної інформації, її збереження, конфіденційності та використання в інтересах

національної безпеки України, аналізу на її основі стану і тенденції розвитку подій, що відбуваються в Україні і в світі;

– визначення потенційних та реальних загроз національним інтересам України.

Рада національної безпеки і оборони України проводить роботу, щодо виявлення і оцінки загроз інформаційній безпеці та готує проекти рішень Президента України щодо запобігання цим загрозам, розробляє пропозиції у галузі забезпечення інформаційної безпеки.

Рада національної безпеки і оборони України здійснює поточний контроль за діяльністю органів виконавчої влади у сфері інформаційної безпеки, подає Президентові України відповідні висновки та пропозиції.

Указом Президента України у 2002 р. при РНБО було створено Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки, яка є консультативно-дорадчим органом із зазначених питань.

У складі апарату РНБО функціонує служба з питань інформаційної безпеки та кібербезпеки.

У структурі Офісу Президента України функціонує Директорат інформаційної політики.

Кабінет Міністрів України як вищий орган у системі органів виконавчої влади, відповідальний перед Президентом України та підконтрольний і підзвітний Верховній Раді України у межах, передбачених Конституцією України. Відповідно до ст. 116 Конституції України:

– забезпечує інформаційний суверенітет України, здійснення внутрішньої і зовнішньої інформаційної політики держави, виконання Конституції і законів України, актів Президента України, що стосуються інформаційної безпеки;

– вживає заходів щодо забезпечення прав і свобод людини і громадянина в інформаційній сфері;

– забезпечує проведення державної політики інформаційної безпеки;

– спрямовує і координує роботу усієї системи органів державного управління з питань, що стосуються інформаційної безпеки.

Окрім цього Кабінет Міністрів України:

– визначає потреби в витратах на забезпечення інформаційної безпеки, забезпечує виконання затвердженого Верховною Радою України Державного бюджету України щодо фінансування заходів у сфері інформаційної безпеки у визначених обсягах;

– організовує розроблення і виконання державних програм з розвитку інформаційної інфраструктури органів державного управління;

– здійснює передбачені законодавством заходи щодо формування, розміщення, фінансування та виконання державного оборонного замовлення на поставку (закупівлю) продукції, виконання робіт, надання послуг для потреб органів, що забезпечують інформаційну безпеку;

– встановлює порядок надання суб’єктам забезпечення інформаційної безпеки у користування державного майна, засобів зв’язку і радіочастотного ресурсу, комунікацій, інших об’єктів інфраструктури держави, навігаційної, топогеодезичної, метеорологічної, гідрографічної та іншої інформації;

– здійснює загальнодержавні заходи щодо забезпечення живучості об’єктів інформаційної інфраструктури;

– забезпечує комплектування особовим складом сили забезпечення інформаційної безпеки;

– утворює, реорганізовує, ліквідовує науково-дослідні установи, навчальні заклади та окремі кафедри (відділення, факультети) суб’єктів забезпечення інформаційної безпеки;

– забезпечує реалізацію права на соціально-економічний захист відповідно до законодавства України, що регламентує діяльність окремих суб’єктів забезпечення інформаційної безпеки;

– здійснює у визначених законом випадках регулювання господарської діяльності у суб'єктах забезпечення інформаційної безпеки;

– встановлює відповідно до закону порядок реалізації та утилізації об'єктів інформаційної інфраструктури, інформаційних ресурсів тощо.

Національна рада України з питань телебачення і радіомовлення є постійно діючим колегіальним органом, метою діяльності якого є нагляд за дотриманням законів України у сфері телерадіомовлення, а також здійснення регуляторних повноважень.

Відповідно до законодавства Національна рада здійснює наглядові, регуляторні повноваження та повноваження щодо організації та перспектив розвитку телерадіомовлення.

Наглядові повноваження Національної ради:

– нагляд за дотриманням телерадіоорганізаціями та провайдерами програмної послуги вимог законодавства у галузі телерадіомовлення, в тому числі реклами та спонсорства;

– нагляд за дотриманням ліцензіатами ліцензійних умов та умов ліцензій, стандартів та норм технічної якості телерадіопрограм, визначеного законодавством порядку мовлення під час проведення виборчих кампаній та референдумів;

– нагляд за дотриманням телерадіоорганізаціями законодавства України у сфері кінематографії, вимог щодо частки вітчизняного продукту у їх програмах (передачах) та вживання мов при здійсненні телерадіомовлення;

– нагляд за дотриманням телерадіоорганізаціями законодавства у сфері захисту суспільної моралі;

– нагляд за дотриманням телерадіоорганізаціями вимог законодавства щодо складу їх засновників (власників), а також частки іноземних інвестицій у їх статутному капіталі;

– застосування в межах своїх повноважень санкцій відповідно до закону (оголошення попередження, штраф, звернення до суду із заявою про анулювання ліцензії);

– офіційний моніторинг телерадіопрограм тощо.

Регуляторні повноваження Національної ради:

– ліцензування телерадіомовлення та провайдерів програмної послуги;

– участь у розробленні та погодження проекту Національної таблиці розподілу смуг радіочастот України і Плану використання радіочастотного ресурсу України у частині смуг радіочастот, виділених для потреб телерадіомовлення;

– розроблення умов використання та визначення користувачів радіочастотного ресурсу, виділеного для потреб телерадіомовлення;

– забезпечення і сприяння конкуренції у діяльності телерадіо-організацій усіх форм власності відповідно до вимог законодавства, створення умов щодо недопущення усунення, обмеження чи спотворення конкуренції в телерадіоінформаційному просторі;

– ведення Державного реєстру телерадіоорганізацій України.

Повноваженнями Національної ради щодо організації та перспектив розвитку телерадіомовлення є:

– участь у розробці і реалізації державної політики у сфері телерадіомовлення;

– розробка і затвердження Плану розвитку національного телерадіоінформаційного простору;

– сприяння включенню телерадіоорганізацій України до світового інформаційного простору і здійсненню їх діяльності відповідно до міжнародних стандартів та інші.

Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг

поштового зв'язку, є центральним органом виконавчої влади із спеціальним статусом, який утворюється Кабінетом Міністрів України.

Особливості спеціального статусу регуляторного органу – Національної комісії – обумовлюються його завданнями і повноваженнями, які визначаються законодавством України; здійснює заходи щодо сприяння адаптації (гармонізації) законодавства України у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку до законодавства Європейського Союзу.

Основними завданнями Національної комісії є:

1) створення умов для ефективного функціонування та розвитку сфер електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку;

2) сприяння відкриттю ринків у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку для всіх споживачів і постачальників та забезпечення недискримінаційного доступу користувачів до електронних комунікаційних послуг та послуг поштового зв'язку;

3) сприяння взаємовигідній інтеграції ринків електронних комунікацій та надання послуг поштового зв'язку України з відповідними ринками інших держав, зокрема в рамках Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони;

4) забезпечення захисту прав споживачів щодо отримання послуг належної якості відповідно до вимог законодавства;

5) забезпечення інвестиційної привабливості розвитку інфраструктури, ринків у сферах електронних комунікацій та надання послуг поштового зв'язку;

6) сприяння розвитку конкуренції на ринках електронних комунікацій та надання послуг поштового зв'язку;

7) забезпечення дотримання принципів управління радіочастотним спектром;

8) інші завдання, передбачені законами України «Про електронні комунікації», «Про поштовий зв'язок», «Про доступ до об'єктів будівництва, транспорту, електроенергетики з метою розвитку електронних комунікаційних мереж», «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» та іншими законодавчими актами, що регулюють відносини у відповідних сферах.

Державний комітет телебачення і радіомовлення України (Держкомтелерадіо) є центральним органом виконавчої влади із спеціальним статусом, діяльність якого спрямовується і координується Кабінетом Міністрів України через Міністра культури та інформаційної політики, бере участь у забезпеченні формування та реалізує державну політику у сфері телебачення і радіомовлення, інформаційній та видавничій сфері.

Держкомтелерадіо відповідно до покладених на нього завдань:

– бере участь у законотворчій діяльності з питань, що належать до його компетенції;

– виконує разом з іншими державними органами завдання щодо забезпечення інформаційної безпеки, розробляє заходи щодо запобігання внутрішньому і зовнішньому інформаційному впливу, який загрожує інформаційній безпеці держави, суспільства, особи;

– визначає порядок функціонування та проводить моніторинг інформаційного наповнення веб-сайтів та стан роз'яснювальної роботи органів виконавчої влади з пріоритетних питань державної політики та надає пропозиції зазначеним органам;

– аналізує та прогнозує розвиток ринку у сфері телебачення і радіомовлення, інформаційній та видавничій сфері, поліграфії;

– сприяє розвитку вітчизняних засобів масової інформації, книговидавничої справи та книгорозповсюдження, підвищенню художньої якості вітчизняних телерадіопрограм, захисту суспільства від негативного впливу аудіо- і відеопродукції, яка становить загрозу суспільній моралі;

– забезпечує дотримання державної мовної політики у сфері телебачення і радіомовлення, інформаційній та видавничій сфері;

– сприяє створенню та діяльності Суспільного телебачення і радіомовлення, впровадженню ефірного наземного цифрового телерадіомовлення;

– здійснює методологічне забезпечення та координує діяльність державних телерадіоорганізацій, інформаційних агентств, видавництв, поліграфічних підприємств і підприємств книгорозповсюдження, установ та організацій;

– є замовником на виробництво і розповсюдження теле- та радіопрограм, випуск видавничої продукції, проведення наукових досліджень у сфері засобів масової інформації, книговидавничої справи та інформаційно-бібліографічної діяльності;

– забезпечує в межах повноважень міжнародне співробітництво, бере участь у розробленні проектів та укладенні міжнародних договорів України, забезпечує їх виконання.

Міністерство культури та інформаційної політики України є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сферах культури, державної мовної політики, популяризації України у світі, державного іномовлення, інформаційного суверенітету України (у частині повноважень з управління цілісними майновими комплексами державного підприємства

“Мультимедійна платформа іномовлення України” та Українського національного інформаційного агентства “Укрінформ”) та інформаційної безпеки.

Міністерство культури та інформаційної політики України відповідно до покладених на нього завдань:

– узагальнює практику застосування законодавства з питань, що належать до його компетенції та розробляє проекти законів та інших нормативно-правових актів;

– здійснює нормативно-правове регулювання у сферах культури та мистецтв, інформаційного суверенітету, інформаційної безпеки, в інформаційній та видавничій сферах, у сфері телебачення і радіомовлення;

– визначає перспективи та пріоритетні напрями розвитку у сферах культури та мистецтв, інформаційного суверенітету, інформаційної безпеки, в інформаційній та видавничій сферах, у сфері телебачення і радіомовлення;

– бере участь у формуванні державної інформаційної політики;

– вживає заходів до захисту прав громадян на вільний збір, зберігання, використання і поширення інформації, зокрема на тимчасово окупованих територіях, відповідно до покладених на нього завдань;

– вживає разом з іншими органами державної влади заходів до захисту неповнолітніх від негативного впливу інформаційної продукції, зокрема аудіо- і відеопродукції, яка становить загрозу суспільній моралі або може зашкодити фізичному, психічному чи моральному розвитку неповнолітніх;

– надає методичну та практичну допомогу засобам масової інформації у сфері інформаційного суверенітету України (у частині повноважень з управління цілісними майновими комплексами державного підприємства “Мультимедійна платформа іномовлення України” та Українського національного інформаційного агентства “Укрінформ”) та інформаційної безпеки;

– бере участь у формуванні єдиного інформаційного простору, сприянні розвитку інформаційного суспільства;

– розробляє заходи щодо запобігання внутрішньому і зовнішньому інформаційному впливу, який загрожує інформаційній безпеці держави, суспільства, особи;

– спрямовує і надає методичну та практичну допомогу структурним підрозділам центральних органів виконавчої влади, на які покладається взаємодія із засобами масової інформації;

– визначає порядок функціонування веб-сайтів органів виконавчої влади та подає Кабінетові Міністрів України пропозиції щодо інформаційного наповнення Єдиного веб-порталу органів виконавчої влади;

– проводить моніторинг інформаційного наповнення веб-сайтів органів виконавчої влади та подає пропозиції зазначеним органам;

– розробляє плани заходів щодо сприяння незалежності засобів масової інформації, захисту прав журналістів та споживачів інформаційної продукції;

– організовує проведення досліджень впливу результатів діяльності засобів масової інформації на суспільну свідомість;

– сприяє розбудові в Україні системи державних стратегічних комунікацій;

– сприяє дотриманню в Україні свободи слова;

– розробляє та вносить на розгляд Кабінету Міністрів України програмні документи у сфері захисту інформаційного простору України від зовнішнього інформаційного впливу;

– забезпечує моніторинг інформації у вітчизняних та іноземних засобах масової інформації;

– сприяє популяризації та формуванню позитивного іміджу України у світових інформаційних ресурсах та національних інформаційних ресурсах іноземних держав з метою захисту її політичних, економічних та соціально-

культурних інтересів, зміцнення національної безпеки і відновлення територіальної цілісності України;

– здійснює міжнародне співробітництво, забезпечує виконання зобов'язань, взятих за міжнародними договорами України, з питань державного іномовлення, інформаційної безпеки та стратегічних комунікацій, тощо.

Міністерство цифрової трансформації України є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики:

– у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації;

– у сфері впровадження електронного документообігу;

– у сфері розвитку цифрових навичок та цифрових прав громадян;

– у сферах відкритих даних, публічних електронних реєстрів, розвитку національних електронних інформаційних ресурсів та інтероперабельності, розвитку інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу;

– у сфері надання електронних та адміністративних послуг;

– у сферах електронних довірчих послуг та електронної ідентифікації;

– у сфері розвитку ІТ-індустрії;

– у сфері розвитку та функціонування правового режиму Дія Сіті;

Забезпечує виконання функцій центрального засвідчувального органу.

Міністерство цифрової трансформації України бере участь у:

– формуванні державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних

інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку;

– розроблення норм, стандартів у сферах електронних довірчих послуг, електронної ідентифікації та автентифікації;

– розроблення критеріїв і порядку проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах; організації та проведенні оцінки стану захищеності державних інформаційних ресурсів, наданні відповідних рекомендацій;

– розроблення та впровадження вимог:

до форматів даних електронного документообігу в державних органах;

щодо функціонування електронного документообігу;

до оформлення документів, організації документообігу, зокрема електронного документообігу;

– розроблення та організації виконання державних програм з питань захисту інформації та кіберзахисту;

– здійснення заходів щодо забезпечення функціонування Національної системи конфіденційного зв'язку та Національної телекомунікаційної мережі;

– здійснює моніторинг даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також про їх наслідки, інформує правоохоронні органи для вжиття заходів із запобігання та припинення злочинів у зазначеній сфері;

– здійснює визначені законом повноваження у сферах електронних довірчих послуг та електронної ідентифікації та ін..

Державна служба спеціального зв'язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону.

Державна служба спеціального зв'язку та захисту інформації України спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки і оборони України.

Основними завданнями Державної служби спеціального зв'язку та захисту інформації України є:

– формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі - інформаційно-комунікаційні системи) і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, активної протидії агресії у кіберпросторі;

– участь у формуванні та реалізації державної політики у сферах електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування), електронної ідентифікації (з використанням електронних довірчих послуг, захисту критичної інформаційної інфраструктури), електронних довірчих послуг, захисту критичної інформаційної інфраструктури (у частині встановлення вимог з безпеки та захисту інформації під час надання та використання електронних довірчих послуг, захисту критичної інформаційної інфраструктури, контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг, захисту критичної інформаційної інфраструктури);

– забезпечення в установленому порядку та в межах компетенції діяльності суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом;

– реалізація державної політики щодо захисту критичної технологічної інформації, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснення державного контролю в цих сферах;

– визначення вимог до захисту критичної технологічної інформації, формування загальних вимог до кіберзахисту об'єктів критичної інфраструктури, ведення переліку об'єктів критичної інформаційної інфраструктури, здійснення заходів щодо його оновлення та актуалізації;

– створення та забезпечення функціонування системи активної протидії агресії у кіберпросторі;

– створення та забезпечення функціонування Центру активної протидії агресії у кіберпросторі;

– виконання інших завдань, передбачених законодавством у сфері забезпечення кібербезпеки та кіберзахисту.

Служба безпеки України – державний орган спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України та підпорядкована Президенту України.

На Службу безпеки України покладається у межах визначеної законодавством компетенції захист державного суверенітету, конституційного ладу, територіальної цілісності, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці. До завдань Служби безпеки України також входить попередження, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, тероризму та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України.

Служба безпеки України відповідно до своїх основних завдань зобов'язана:

– здійснювати контррозвідувальні заходи з метою попередження, виявлення, припинення і розкриття будь-яких форм розвідувально-підривної діяльності проти України;

– забезпечувати захист державного суверенітету, конституційного ладу і територіальної цілісності України від протиправних посягань з боку окремих осіб та їх об'єднань;

– здійснювати відповідно до законодавства профілактику правопорушень у сфері державної безпеки;

– здійснювати функцію технічного регулювання у сфері спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації та інші.

До складу Центрального управління СБУ входять підрозділи, які виконують повноваження у сфері забезпечення інформаційної безпеки країни: *Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, Департамент охорони державної таємниці та*

ліцензування, Департамент захисту національної державності, Ситуаційний центр забезпечення кібербезпеки.

На базі Ситуаційного центру забезпечення кібербезпеки СБУ функціонує система управління подіями інформаційної безпеки (SIEM), яка моніторить події в режимі реального часу та дозволяє аналізувати стан інформаційної безпеки. Потенційно критичні події безпосередньо обробляються аналітиками безпеки, що дає змогу оперативно виявляти, реагувати та попереджувати загрози в національному кіберпросторі.

Міністерство внутрішніх справ України – центральний орган виконавчої влади України, діяльність якого спрямовується і координується Кабінетом Міністрів України.

МВС України є головним (провідним) органом у системі центральних органів виконавчої влади з питань формування і реалізації державної політики у сфері забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку, а також надання поліцейських послуг; захисту державного кордону, цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню; міграції та протидії нелегальній міграції, громадянства тощо.

У складі МВС України функціонує *Національна поліція*, яка як центральний орган виконавчої влади, служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку.

Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної

політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність.

Основні завдання Департаменту кіберполіції Національної поліції України:

– участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– реалізація державної політики в сфері протидії кіберзлочинності;

– завчасне інформування населення про появу нових кіберзлочинців;

– упровадження програмних засобів для систематизації кіберінцидентів;

– реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної Цілодобової мережі контактних пунктів;

– сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень.

Міністерство оборони України забезпечує виконання вимог законодавства України, здійснює реалізацію концепцій, програм у сфері інформаційної безпеки.

Департамент охорони державної таємниці – структурний підрозділ Міністерства оборони, який забезпечує та здійснює контроль за дотримання вимог щодо охорони державної таємниці у структурі Міністерства оборони та підпорядкованих йому організацій.

Головне управління розвідки Міністерства оборони України згідно із Законом України «Про розвідку» здійснює розвідувальну діяльність у

воєнній сфері, сферах оборони, військового будівництва, військово-технічній та кібербезпеки.

На розвідувальний орган Міністерства оборони України покладаються такі завдання:

– добування, аналітичне опрацювання та надання органам державної влади розвідувальної інформації;

– проводять заходи з метою сприяння реалізації національних інтересів України, забезпечення безпеки та участі у формуванні та реалізації державної політики у визначених законом сферах, посилення обороноздатності держави, економічного та науково-технічного розвитку;

– виявляють і визначають ступінь зовнішніх загроз національній безпеці України, у тому числі у кіберпросторі, життю, здоров'ю її громадян та об'єктам державної власності за межами України, організовують і проводять спеціальні (активні) заходи щодо таких загроз і з протидії іншій діяльності, що становить зовнішню загрозу національній безпеці України;

– беруть участь у боротьбі з тероризмом, протидії розвідувально-підривній діяльності проти України, транснаціональній організованій злочинності та іншій злочинній діяльності, що становлять зовнішню загрозу національній безпеці України;

– здійснюють співробітництво з компетентними органами іноземних держав, міжнародними організаціями;

– здійснюють інші визначені законом функції з метою забезпечення національної безпеки України.

– здійснення спеціальних заходів, спрямованих на підтримку національних інтересів і державної політики України в економічній, політичній, воєнній, військово-технічній, екологічній та інформаційній сферах, зміцнення обороноздатності, економічного і науково-технічного розвитку, захисту та охорони державного кордону;

Генеральний штаб Збройних Сил України - головний військовий орган з планування оборони держави, управління застосуванням Збройних сил України, координації та контролю за виконанням завдань у сфері оборони іншими утвореними відповідно до законів України військовими формуваннями, органами виконавчої влади, органами місцевого самоврядування, правоохоронними органами, Державною спеціальною службою транспорту і Державною службою спеціального зв'язку та захисту інформації України.

Головне управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України є структурним підрозділом Генерального штабу Збройних Сил України і призначене для проведення єдиної державної технічної політики в сфері зв'язку та інформатизації, захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах Збройних Сил України та організації зв'язку.

Окрім того, виконання завдань та програм в інформаційній сфері здійснюють понад *20 інших центральних органів виконавчої влади*: Міністерство юстиції України, Міністерство закордонних справ України, Міністерство освіти і науки України, Міністерство інфраструктури України, Державна архівна служба України тощо.

На рівні адміністративно-територіальних одиниць України повноваження з питань інформаційної політики та забезпечення інформаційної безпеки виконують *місцеві органи виконавчої влади* та *органи місцевого самоврядування*.

Органи судочинства. Судочинство в Україні здійснюється виключно судами на засадах верховенства права, забезпечення кожному права на справедливий суд та повагу до інших прав і свобод, які гарантують Конституція та закони України, а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Суди відповідно до ст. 6 Конституції є самостійною гілкою влади і діють незалежно від законодавчої і виконавчої влади. Юрисдикція судів поширюється на всі правовідносини, що виникають у державі.

Система правосуддя має на меті постійно і надійно захищати громадян, підприємства, організації від протиправних посягань, зловживань влади, гарантувати їм дієве поновлення порушених законних прав і свобод.

Відповідно до закону діють апеляційні та місцеві суди. Вищими судовими органами спеціалізованих судів є відповідні вищі суди. Найвищим судовим органом у системі судів загальної юрисдикції є Верховний Суд України.

Судова влада виступає в ролі арбітра, що вирішує спори: між громадянами, громадянами і підприємствами, громадянами і державними чи громадськими організаціями, між громадянами і державою в цілому тощо.

Суди зобов'язані своєчасно й дієво захищати права та свободи громадян, підприємств, організацій шляхом розгляду цивільних, господарських, адміністративних, кримінальних справ і справ про адміністративні правопорушення. Суд не може відмовити у правосудді, якщо суб’єкт вважає, що його права і свободи порушені або створюються перешкоди для їх реалізації чи мають місце інші порушення прав і свобод.

Конституція України встановлює, що носієм суверенітету і єдиним джерелом влади в Україні є народ, а громадяни мають право брати участь в управлінні державними справами.

Громадяни та організації громадянського суспільства можуть залучатися до процесу державного управління через такі механізми громадської участі як інформування (висвітлення діяльності органів влади на сайтах, у друкованих та Інтернет-виданнях тощо), консультації (інтерактивні методи обговорення на всіх етапах прийняття управлінських рішень, вивчення громадської думки) та механізми прийняття рішень (облік та

використання пропозицій громадськості при прийнятті управлінських рішень).

Одним з найбільш поширених та дієвих механізмів активної участі громадськості в публічному управлінні є *діяльність громадських рад* при органах державної влади, органах місцевого самоврядування, які представляють та захищають інтереси громадян у процесі підготовки, обговорення та прийняття державно-управлінських рішень з найважливіших питань життя суспільства і держави, а також є суб'єктами здійснення громадського контролю за діяльністю органів виконавчої влади, органів місцевого самоврядування.

Громадська рада відповідно до покладених на неї завдань:

– готує та подає органу влади пропозиції щодо орієнтовного плану проведення консультацій з громадськістю, організації консультацій та питань, які обговорюватимуться;

– проводить відповідно до законодавства громадську експертизу діяльності органу та громадську антикорупційну експертизу нормативно-правових актів та проектів нормативно-правових актів, які розробляє орган;

– здійснює громадський контроль за врахуванням органом пропозицій та зауважень громадськості, забезпечення ним прозорості та відкритості своєї діяльності, доступу до публічної інформації, яка знаходиться у його володінні, а також дотриманням ним нормативно-правових актів, спрямованих на запобігання та протидію корупції;

– інформує в обов'язковому порядку громадськість про свою діяльність, прийняті рішення та їх виконання;

– збирає, узагальнює та подає органу інформацію про пропозиції інститутів громадянського суспільства щодо вирішення питань, які мають важливе суспільне значення;

– організовує публічні заходи для обговорення актуальних питань.

Для прикладу можна навести *Громадську раду з питань свободи слова та інформації*, яка є постійно діючим незалежним громадським колегіальним експертним органом *при Комітеті Верховної Ради України з питань свободи слова та інформації*. Громадська рада здійснює координацію у сфері співпраці недержавних організацій та експертів з Комітетом. Основними цілями діяльності Громадської ради є забезпечення права на свободу слова та права на інформацію, реформування національного інформаційного законодавства.

До складу громадських рад при органах виконавчої влади можуть входити представники не тільки громадських об'єднань, але й релігійних, благодійних організацій, творчих спілок, професійних спілок та їх об'єднань, асоціацій, організацій роботодавців, органів самоорганізації населення, недержавних засобів масової інформації, інших непідприємницьких товариств та установ.

Питання для самоконтролю

Назвіть міжнародні організації, що займаються питаннями нормативного забезпечення інформаційної безпеки на глобальному рівні.

Назвіть основні міжнародні документи, які прийняті за результатами роботи міжнародних організацій.

Які міжнародні стандарти у сфері інформаційної безпеки ви знаєте?

Опишіть структуру вітчизняної нормативно-правової бази у сфері забезпечення інформаційної безпеки? Назвіть основні законодавчі акти з інформаційної безпеки України.

Роль Верховної Ради України та її профільних комітетів у забезпеченні інформаційної безпеки держави? Назвіть комітети Верховної Ради України, до повноважень яких входять питання забезпечення інформаційної безпеки.

Зазначте повноваження Уповноваженого Верховної Ради України з прав людини у сфері забезпечення інформаційної безпеки.

Назвіть повноваження у сфері інформаційної безпеки держави покладено на Раду національної безпеки та оборони України?

Охарактеризуйте систему органів виконавчої влади, які виконують завдання із забезпечення інформаційної безпеки держави.

Які регуляторні органи виконавчої влади з питань інформаційної безпеки держави ви знаєте? Зазначте їхні основні функції.

Якою є роль організацій громадянського суспільства, громадян у забезпеченні інформаційної безпеки країни?

Тема 4. ДЕРЖАВНА ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. Розглядаючи сутність державної політики інформаційної безпеки, насамперед встановимо значення поняття «державна політика». У наукових дослідженнях з державного управління представлено декілька підходів до визначення державної політики.

На думку авторів словника-довідника «Державне управління», державна політика є засобом, що дозволяє державі досягнути певної мети в конкретній галузі, використовуючи правові, економічні, адміністративні методи впливу, спираючись на ресурси, які є в її розпорядженні.

Відповідно до іншого підходу державна політика включає визначення проблеми, цілей та інструментів розв'язання проблеми.

Натомість автори Енциклопедичного словника з державного управління вважають, що державна політика – це дії системи органів державної влади згідно з визначеними цілями, напрямами, принципами для розв'язування сукупності взаємопов'язаних проблем у певній сфері суспільної діяльності.

Таким чином державна політика включає як визначення системи напрямів, методів, завдань щодо досягнення певної мети (теоретична складова), так і комплекс дій, заходів для її втілення в життя (практична складова). Тобто можна говорити про вироблення державної політики як сукупності цілей, завдань, засобів і про реалізацію державної політики – комплексу дій, які практично здійснюються органами державної влади.

З'ясуємо сутність понять «державна інформаційна політика» та «державна політика інформаційної безпеки».

Відповідно до Закону України «Про інформацію» державна інформаційна політика – це сукупність основних напрямів і способів діяльності держави з одержання, використання, поширення та зберігання інформації.

Концепція національної інформаційної політики України визначає національну інформаційну політику як стратегію, напрями і завдання держави у сфері збирання, зберігання, використання та поширення інформації та інформаційних ресурсів у суспільстві.

Отже, державна політика інформаційної безпеки (забезпечення інформаційної безпеки) - сукупність основних напрямів і способів діяльності держави щодо забезпечення:

- інформаційного суверенітету держави,
- захищеності життєво важливих інтересів особистості, суспільства й держави від негативних інформаційних впливів у всіх сферах життєдіяльності,
- розвитку й захисту всіх елементів національного інформаційного простору, в тому числі інфраструктури та ресурсів,
- захищеності громадян і суспільства загалом від маніпулювання інформацією та негативних інформаційно-психологічних впливів,
- здатності держави запобігати, нейтралізувати чи послаблювати дію внутрішніх і зовнішніх інформаційних загроз як технічного, так і соціально-психологічного характеру.

Забезпечення інформаційної безпеки України має здійснюватися за такими принципами:

- свобода збирання, зберігання, використання та поширення інформації;
- достовірність, повнота та неупередженість інформації;
- обмеження доступу до інформації виключно на підставі закону;

- гармонізація особистих, суспільних і державних інтересів;
- запобігання правопорушенням в інформаційній сфері;
- економічна доцільність;
- гармонізація українського законодавства в інформаційній сфері з міжнародним; пріоритетність національної інформаційної продукції.

Крім того необхідним є використання комплексного підходу до вирішення проблем забезпечення інформаційної безпеки.

Основними засобами досягнення цілей політики інформаційної безпеки України мають бути:

- створення законодавчої та нормативної баз;
- визначення компетенцій органів державної влади та управління;
- здійснення моніторингу інформаційної безпеки з метою аналізу та розробки заходів задля усунення недоліків та подальшого удосконалення системи забезпечення інформаційної безпеки;
- здійснення контролю за діяльністю юридичних та фізичних осіб у сфері забезпечення інформаційної безпеки;
- фінансова, наукова та матеріально-технічна підтримка юридичних та фізичних осіб, що беруть участь у створенні системи забезпечення інформаційної безпеки;
- стандартизація, сертифікація та ліцензування діяльності в сфері забезпечення інформаційної безпеки;
- удосконалення та розвиток державної інформаційної інфраструктури, в тому числі інформаційних ресурсів з урахуванням вимог інформаційної безпеки;
- удосконалення системи підготовки інтелектуальної еліти суспільства та створення умов для її творчої роботи;
- удосконалення системи освіти та наукової діяльності, а також виховання з урахуванням вимог інформаційної безпеки тощо.

У науці представлено багато бачень щодо напрямів, методів, засобів забезпечення інформаційної безпеки держави. Відомим є поділ усіх засобів та методів забезпечення інформаційної безпеки на нормативно-правові, організаційні та програмно-технічні. Деякі фахівці розглядають це питання детальніше і виділяють крім вище зазначених методи й засоби кадрового, інформаційно-аналітичного, матеріально-технічного, фінансового забезпечення. Відзначено також приналежність до засобів забезпечення інформаційної безпеки держави і зовнішньо-політичних та військових засобів.

Цікавою є схема напрямів та засобів забезпечення інформаційної безпеки держави із відзначенням взаємозв'язків між ними, представлена закордонними науковцями (Рис. 1)

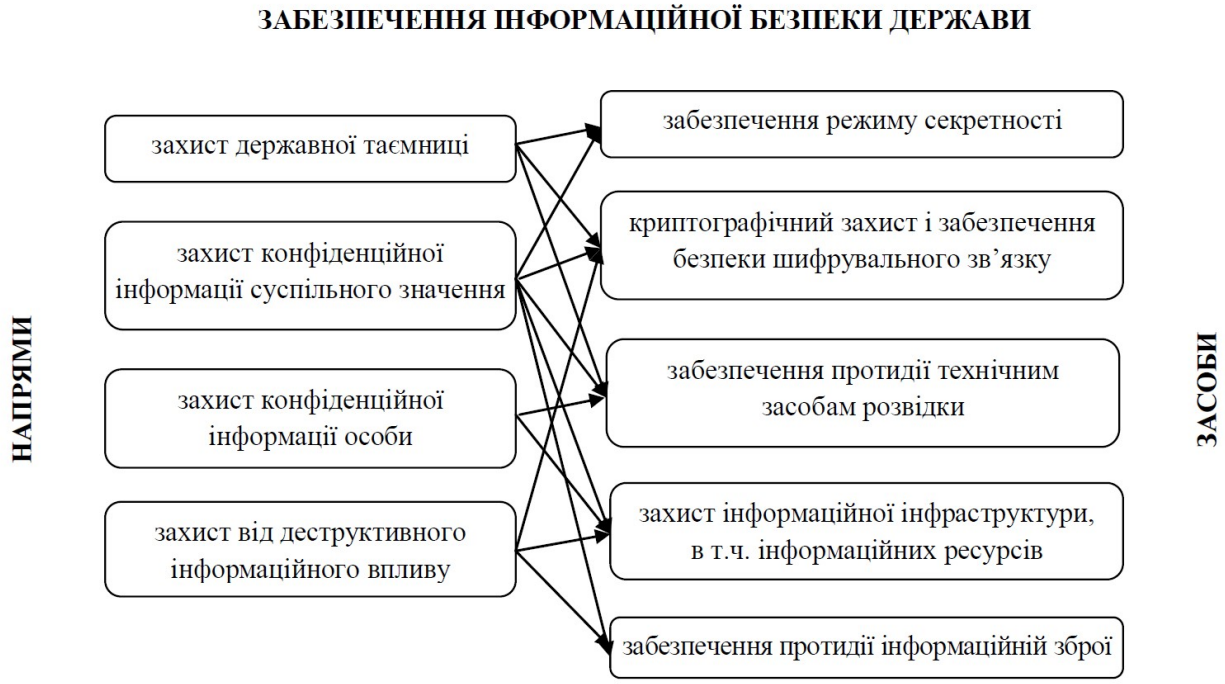


Рис. 1. Напрями та засоби забезпечення інформаційної безпеки держави.

Відповідно до іншого бачення, діяльність із забезпечення інформаційної безпеки держави можна поділити на три основні напрями: державно-управлінський, техніко-технологічний та соціально-змістовний.

Державно-управлінський напрям:

- реалізація державної політики інформаційної безпеки та забезпечення інформаційного суверенітету України;

- законодавче визначення стратегічних напрямів забезпечення інформаційної безпеки та їх реалізація;

- удосконалення державного регулювання розвитку інформаційної сфери, протидія її монополізації;

- належне інформаційне забезпечення прийняття державно-управлінських рішень;

- постійна відкрита інформаційна взаємодія між державною владою і громадянським суспільством (е-уряд, е-демократія);

- забезпечення урядового зв'язку і Національної системи конфіденційного зв'язку;

- участь у міжнародному співробітництві у сфері інформаційної безпеки;

- протидія поширенню інформації, що містить заклики до зміни конституційного ладу та кордонів держави, міжнаціональної та міжконфесійної ворожнечі;

- запобігання та протидія інформаційній експансії інших держав, інформаційному тероризму, використанню інформаційної зброї;

- ведення активної розвідувальної, контррозвідувальної і оперативно-розшукової діяльності з метою забезпечення інформаційної безпеки.

Техніко-технологічний напрям:

- забезпечення інноваційного потенціалу країни через впровадження новітніх технологій в інформаційній сфері;

- підтримка вітчизняних виробників засобів інформатизації та захисту інформації, створення передумов для підвищення їх конкурентоспроможності на світовому та національному ринках;

- стандартизація, сертифікація і ліцензування засобів інформатизації та захисту інформації;

- розвиток національного інформаційного простору, створення умов для його інтегрування у світовий інформаційний простір;

- розвиток, ефективне використання та захист національної інформаційної інфраструктури;

- розвиток, ефективне використання та захист інформаційних ресурсів, забезпечення вільного доступу до них, формування системи національних електронних ресурсів;

- управління вітчизняним сегментом мережі Інтернет;

- технічний та криптографічний захист інформації з обмеженим доступом (службової інформації та інших видів конфіденційної інформації, державної таємниці);

- запобігання та протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам.

Соціально-змістовний напрям:

- наповнення національного інформаційного простору якісним вітчизняним інформаційним продуктом, забезпечення потреб громадян у якісній, повній і достовірній інформації для їх життєдіяльності, освіти та розвитку;

- поширення у світовому інформаційному просторі достовірної інформації про Україну, розвиток іномовлення;

- забезпечення законності та незалежності функціонування ЗМІ, запобігання їх монополізації;

- реалізація конституційних прав і свобод громадян на вільне збирання, зберігання, використання та поширення інформації, свободу думки й слова, вільне вираження своїх поглядів і переконань;

- захист від маніпулювання інформацією та дезінформування, деструктивних впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому;

- забезпечення приватності життя громадян, захист персональних даних;

- захист суспільної моралі, духовної, культурної і мовної самобутності;

- запобігання та протидія поширенню інформації, що пропагує агресію, насильство, наркоманію, алкоголізм та інші негативні суспільні явища.

У грудні 2021 року Указом Президента України було схвалено Стратегію інформаційної безпеки, яка на період до 2025 року визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних.

Посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина є метою державної політики забезпечення інформаційної безпеки..

Досягнення мети здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між

органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки.

Питання для самоконтролю

Що таке державна інформаційна політика?

Назвіть основні завдання державної інформаційної політики.

Що таке державна політика інформаційної безпеки?

Назвіть завдання державної політики інформаційної безпеки.

Вкажіть відмінності між поняттями «державна інформаційна політика» та «державна політика інформаційної безпеки».

Тема 5. БЕЗПЕКА ІНФОРМАЦІЇ, ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Інформація, інформаційні відносини, інформаційні ресурси

Інформація (від латинського слова «informacio» - роз'яснення, виклад) – це відомості (або їх сукупність) про предмети, явища і процеси оточуючого нас світу. Інформація – це абстрактне поняття. Інформація не існує сама по собі – вона укладена в структурі об'єкта або системи, в знаках і символах, зафіксованих на матеріальних носіях. Інформація проявляється в інформаційних процесах в природі, в суспільстві і техніці, а також в процесі розумової діяльності людини щодо сприйняття навколишньої дійсності.

Законом України «Про інформацію» закріплено таке визначення «***інформація*** - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді».

До основних ознак інформації відносять:

- невичерпність. Інформація є невичерпною, тиражується, але не витрачається, може поширюватися в необмеженій кількості екземплярів практично без зміни її змісту і втрати якості, може належати багатьом особам, може бути використана необмежену кількість разів;
- вимірність. Інформація може бути кількісно виміряна (кількість символів, знаків);
- двоєдинство інформації та її носія. Інформація передається і поширюється в більшості випадків на матеріальному носії і за допомогою матеріального носія;
- фізична невідчужуваність інформації від її творця, власника, споживача;
- наявність організаційної форми, структури у вигляді інформаційних систем, документів, бібліотек тощо;

- цінність. Інформація має певну цінність (може продаватися);
- поширюваність. Інформація не локалізована в просторі, може легко розповсюджуватися.

Серед основних властивостей інформації виділяють: об'єктивність, достовірність, повнота, точність, актуальність, корисність, цінність, зрозумілість, доступність, стислість тощо.

Інформаційні відносини – суспільні відносини, які виникають при збиранні, одержанні, зберіганні, використанні, поширенні та захисту інформації.

Основними принципами інформаційних відносин є:

– гарантованість права на інформацію;

– відкритість, доступність інформації, свобода обміну інформацією;

– достовірність і повнота інформації;

– свобода вираження поглядів і переконань;

– правомірність одержання, використання, поширення, зберігання та захисту інформації;

– захищеність особи від втручання в її особисте та сімейне життя.

Виникнення такого принципово нового поняття як ***інформаційні ресурси*** пов'язано із зростаючою залежністю від наявності інформації, рівня розвитку та ефективності використання засобів її обробки та передачі.

В умовах формування інформаційного суспільства інформаційні ресурси набувають першорядної значимості і прирівнюються до капіталу.

В науці представлено декілька підходів до розуміння сутності інформаційних ресурсів. Зокрема, під інформаційними ресурсами мають на увазі сукупність даних, організованих для отримання достовірної інформації в різних областях знань і практичної діяльності, або особливий вид ресурсів, що ґрунтуються на ідеях і знаннях, нагромаджених у результаті науково-

технічної діяльності людей і подані у формі, придатній для збирання, реалізації та відтворення.

Також інформаційні ресурси розглядають як складову інфраструктури інформаційного простору, що поєднує в собі дані, їхнє місце (засіб) зберігання, взаємозв'язок між інформаційними елементами, відомості про процеси надходження, зберігання, обробки тощо.

Зміст інформаційного ресурсу ми пропонуємо розглядати у двох аспектах: як процес поступового розвитку інформаційної сфери, та як продукт, тобто об'єкт інтелектуальної праці людини. Інформаційним ресурсом є лише та інформація, що актуалізована в суспільстві: входить у систему людської діяльності й має практичне значення для людини як в її соціальному, так і особистому житті.

У вітчизняному законодавстві перше визначення дефініції «інформаційний ресурс» було наведено у Законі України «Про Концепцію Національної програми інформатизації»: «сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо)».

Визначення поняття інформаційних ресурсів наведено в перших статтях Законів «Про науково-технічну інформацію» (1993 р.) та «Про національну програму інформатизації» (1998 р.). Слід зазначити, що мова йде про інформаційні ресурси, які визначаються як документована інформація, що зберігається в різних інформаційних системах (комп'ютерних базах і банках даних, бібліотеках, архівах, інформаційних сховищах тощо). При цьому під документованою розуміється інформація, зафіксована на матеріальному носії з реквізитами, що дозволяють її ідентифікувати (друкована, теле- і радіопродукція державних і інших засобів масової інформації не є предметом даного дослідження).

Інформаційний ресурс має низку характерних особливостей:

– на відміну від інших (матеріальних) ресурсів, він практично невичерпний;

– з використанням ІР не зникає, а зберігається і навіть збільшується;

– застосування нового інформаційного ресурсу замість застарілого потенційно може спричинити дії радикального характеру, багаторазово підвищити продуктивність праці, поліпшити використання інших ресурсів тощо;

– ІР не є самостійним і сам по собі має лише потенційне значення. Тільки поєднуючись з іншими ресурсами – досвідом, працею, кваліфікацією, технікою, енергією, сировиною – він є рушійною силою;

– ефективність застосування ІР пов’язана з ефектом повторного виробництва знань; інформаційна взаємодія дозволяє одержати нові знання ціною менших витрат, порівняно з витратами праці, енергії, часу на його пряме генерування;

– ІР виникають в результаті не просто розумової праці, а її творчої частини.

Сьогодні у наукових та нормативних джерелах представлена велика кількість підходів до класифікації інформаційних ресурсів.

Інформаційні ресурси підрозділяються за класами інформації, що збирається. До первинної інформації, тобто тієї, яка відображає специфіку її джерела, області або сфери створення, виникнення, відноситься інформація, що утворюється самостійно в природних умовах (наприклад, кількість кілець на спилі дерева свідчить про його вік).

Інформація про кількісні та якісні характеристики різних соціальних процесів утворюють клас інформації, яка «знімається». Виділені за цією ознакою інформаційні ресурси можна класифікувати як природні, виробничі, соціально-економічні. Наприклад, інформація про зростання населення.

Інший клас інформаційного ресурсу утворюють відомості, дані, одержані штучно в процесі науково-дослідної діяльності, а також будь-якої творчої роботи. Вона базується на обробці вже наявної інформації зі спеціальним параметрами і моделями (математична обробка, логічна, семантична і т.д.). До цього ж класу відносяться і об'єкти, створені як авторські твори у галузі літератури, мистецтва. Важливим компонентом цих ресурсів є інформація, що отримується в результаті інтелектуальної діяльності людини.

Основні з них подані нижче.

Деякі вчені акцентують на тому, що інформаційний ресурс є симбіозом знань та інформації.

Як відзначалося, інформація – це відомості про суб’єкти, об’єкти, явища і процеси. Знання – сукупність фактів, закономірностей, відносин, евристичних правил, що відбивають рівень знайомства з проблемами деяких предметних галузей.

За європейськими стандартами, знання – це комбінація даних (інформації у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки) та інформації, до яких додається точка зору, навички та досвід експерта, що дає вагомий результат, який може бути використано для прийняття рішень. Знання може бути вичерпним та/або вузьким, індивідуальним та/або колективним.

За іншим визначенням дані – це результат простого збору визначених фактів; інформацією вони стають лише при зв’язуванні у щось корисне, комбінацію хто, що, де і як. У свою чергу знання – це розуміння, як і чому щось відбувається. Українське законодавство взагалі не визначає поняття «знання».

Класифікації інформаційних ресурсів

Критерій	Види ІР
джерело виникнення	– первинні, – вторинні (виникають на основі переробки вже наявної інформації)
вид носія	– паперові, – на машинозчитуваних носіях (кіно-, аудіо-та відеозаписи, електронні), – на каналі зв'язку (ТБ, радіо).
спосіб організації зберігання та використання	– документи на традиційних носіях (книги, газети, журнали), – масив документів, – фонд документів, – архів, – автоматизовані форми.
цільове призначення	масова інформація, бізнес, переписка, особисті, корпоративні, ЗМІ, бізнес, освітні, політика, установи та організації, сервіси та послуги, дошки оголошень, освіта і культура, чати, спорт, відпочинок, зображення і фото, розважальні портали, інші.
зміст	тематична інформація, наукові публікації, рекламна інформація, довідкова інформація, новини, вторинна (бібліографічна) інформація.
сфера життєдіяльності, галузь (ЗУ «Про інформацію»)	– статистичні, – масові (поширювані публічно), – ІР про діяльність державних органів влади та органів місцевого самоврядування, – правові; – ІР про особу; – довідково-енциклопедичні, – соціологічні, – екологічні, – ІР про товар (роботу, послугу); – науково-технічні, – податкові.
обсяг (глобальність)	– глобальні, – загальнонаціональні, – регіональні, – на рівні місцевого самоврядування, соціальних організацій і окремих підрозділів.
джерело	– міжнародні, національні або закордонні,

інформації	– офіційні або неофіційні тощо.
форма власності	– загальнонаціональне надбання, – державна власність, – муніципальна власність, – приватна (особиста, корпоративна) власність.
правовий статус	публічні документи, об'єкти інтелектуальної власності, спам, таємні документи, тощо.
доступ	відкриті або з обмеженим доступом.
мова	англомовні, україномовні, російськомовні тощо.
географічне розташування	європейські, південно-азійські, українські.
важливість	– стратегічні, – тактичні, – операційні.
важливість (міжнародні критерії)	– життєво важливі (пов'язані з виживанням і безпекою нації), – важливі (такі, що здійснюють відчутний вплив на добробут нації та характер міжнародних відносин), – гуманітарні (такі, що безпосередньо не питань свободи, виживання, процвітання нації, але стратегічно й тактично вигідні державі для позитивного позиціонування себе як усередині країни, так і на міжнародній арені).
характер впливу на суспільні процеси	– формувальні (спрямовані на створення суспільних процесів), – стимулювальні (орієнтовані на підтримку та розвиток суспільних процесів), – стримувальні (визначають межі суспільних процесів), – деструктивні, (антиресурс) спрямовані на підрив і усунення визначених процесів).
готовність до використання	– актуальні, – потенційні, – критичні.

В умовах розвитку інформаційного суспільства та інформатизації усіх сфер життєдіяльності суспільства особливого значення набувають електронні інформаційні ресурси.

Електронні інформаційні ресурси – інформаційні ресурси, які зберігають, обробляють, розповсюджують та представляють користувачеві за

допомогою засобів обчислювальної техніки. Їм притаманні такі ознаки: подання інформації в цифровому вигляді (текст, звук, зображення статичне або те, що рухається у цифрових форматах), необхідність програмних та апаратних засобів для її сприйняття людиною (тобто, комп'ютерного обладнання та програмного забезпечення), необхідність телекомунікаційних засобів для отримання або розповсюдження інформації.

У Концепції формування системи національних електронних інформаційних ресурсів визначено, що національні електронні інформаційні ресурси – це «ресурси незалежно від їх змісту, форми, години та місця створення, форми власності, призначені для задоволення потреб громадянина, суспільства, держави. Національні ресурси включають державні, комунальні та приватні ресурси».

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» ***національні електронні інформаційні ресурси*** – це систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів.

До електронних ресурсів відносять:

- електронні текстові аналоги друкованих видань, таких як книги, журнали тощо (при цьому передбачається, що текстова інформація, котра міститься в них, подана у формі, яка допускає посимвольну обробку);

- електронні образи друкованих видань, коли елементи останніх (наприклад, сторінки) подаються як цілісні графічні образи, до цього ж виду електронної інформації належать образи рукописних матеріалів - факсиміле;
- бази даних, які відповідають вимогам до електронної інформації, наприклад, бібліографічні, адресні, статистичні, лінгвістичні, до цього ж виду належать і повнотекстові бази даних, якщо вони не відтворюють повною мірою друковані видання;
- нові форми публікацій, що не мають друкованих аналогів, такі як електронні оголошення, матеріали електронних конференцій та інші електронні повідомлення, доступні користувачам через телекомунікаційні мережі;
- електронні публікації аудіо- та відеоінформації;
- мультимедійні продукти;
- програмні продукти;
- комбіновані програмно-інформаційні продукти, наприклад, геоінформаційні системи;
- електронні ігри.

Види електронних інформаційних ресурсів.

1) Засоби масової інформації. До них відносяться різного роду новинні і семантичні сайти (або електронні версії ЗМІ). Їх відмінною рисою є високий рівень відвідуваності, швидка зміна інформації, наявність відеоряду на сайті.

2) Електронні бібліотеки. Електронна бібліотека – розподілена інформаційна система, що дозволяє надійно зберігати і ефективно використовувати різнорідні колекції електронних документів через глобальні мережі передачі даних в зручному для кінцевого користувача вигляді.

3) Електронні бази даних. У найзагальнішому сенсі база даних - це набір написів і файлів, організованих спеціальним чином. Один з типів баз даних – це документи, набрані за допомогою текстових редакторів і

згруповані за темами. Інший тип - це файли з електронними таблицями, які об’єднані в групи за характером їх використання.

4) Сайти. Корпоративний сайт - це Інтернет-ресурс, присвячений якійсь організації, фірмі, підприємству. Як правило, він знайомить користувачів з фірмою, напрямами і видами її діяльності, відображає різні довідкові матеріали: прайс-листи, умови поставок і оплати; рекламну інформацію: наявність сертифікатів якості, участь у виставках, публікації в пресі тощо; контактну інформацію.

На відміну від корпоративного сайту виділяють персональний і аматорський сайт, домашню сторінку. Вони відрізняються повнотою інформації, що представляється і професіоналізмом виконання.

Як правило, на сайті можна познайомитися з інформацією вузькотематичної спрямованості. Глибина її розкриття може бути різною: від суто ознайомчої, поверхневої до високопрофесійної, що висвітлює всі сторони діяльності. Визначає інформативність сайту його власник. На сайтах може бути представлена велика кількість гіперпосилань, які допомагають орієнтуватися в ньому.

5) Сервіси - це група сайтів, на яких можна скористатися різноманітними сервісними послугами: електронною поштовою скринькою, блогом (а також познайомитися з правилами його ведення), пошуком, різними каталогами, словниками, довідниками, прогнозом погоди, телепрограмою, курсами валют і т. д. Наприклад, Укрнет.

Інформаційний портал - це веб-сайт, організований як багаторівневе об’єднання різних ресурсів і сервісів, оновлення якого відбувається в реальному часі.

Тема 6. НАЦІОНАЛЬНІ ІНФОРМАЦІЙНІ РЕСУРСИ. СИСТЕМА НАЦІОНАЛЬНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Незважаючи на те, що в Україні накопичено велику кількість інформаційних джерел, створено ряд інформаційних центрів, функціонує мережа публічних, наукових й освітніх бібліотек, а обсяги інформації постійно збільшуються, питання формування та використання національних інформаційних ресурсів залишаються постійно актуальними і складними для вирішення.

Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» передбачається, що серед основних напрямів розвитку інформаційного суспільства в Україні слід визначити створення загальнодоступних електронних інформаційних ресурсів на основі врахування національних, світоглядних, політичних, економічних, культурних та інших аспектів розвитку України.

При цьому при створенні загальнодоступних електронних інформаційних ресурсів слід забезпечити генерування національних інформаційних ресурсів в економічній, науково-технічній, соціальній, національно-культурній сферах, охороні довкілля тощо, відповідність електронних інформаційних ресурсів стандартам і технічним регламентам, загальнодержавним, галузевим і локальним класифікаторам і довідникам; створення системи центрів даних, що надають послуги з їхнього зберігання та захисту, збереження в електронному вигляді рідкісних даних, що зберігаються на носіях, які можуть зіпсуватися чи зруйнуватися, із визначенням умов їхнього збереження.

Побіжно Доктрина інформаційної безпеки визначає, що одним з напрямів державної політики у сфері інформаційної безпеки України є розбудова та інноваційне оновлення національних інформаційних ресурсів. При цьому держава з метою забезпечення інформаційної безпеки України

має вживати в економічній сфері таких заходів як формування вітчизняної індустрії інформаційних послуг, підвищення ефективності використання державних, корпоративних і приватних інформаційних ресурсів.

Прийнято низку відповідних актів Кабінету Міністрів України, якими, зокрема, передбачається, що має здійснюватися управління та координація діяльності з питань, пов'язаних з формуванням, використанням і захистом національних ресурсів, включаючи ведення Національного реєстру електронних інформаційних ресурсів.

Національні інформаційні ресурси - вся належна Україні інформація, включаючи окремі документи і масиви документів, незалежно від змісту, форми, часу і місця їх створення, форми власності, а також кінцеві результати інтелектуальної, творчої діяльності, зафіксовані на будь-яких носіях інформації, доступні для використання особою, суспільством і державою через засоби масової інформації та телекомунікації, архіви, бібліотеки, музеї, фонди, банки даних, публічні виступи, художньо-виконавську діяльність тощо.

В іншому визначенні звернуто увагу на аспекти правовласності та вартості національних інформаційних ресурсів України, під якими розуміють окремі документи і масиви документів, результати інтелектуальної, творчої та інформаційної діяльності, бази й банки даних, всі види архівів, бібліотеки, музейні фонди та інші, що містять дані, відомості й знання, зафіксовані на відповідних носіях інформації, є об'єктами права власності всіх суб'єктів України і мають споживацьку вартість (політичну, економічну, соціокультурну, оборонну, історичну, ринкову, інформаційну тощо).

З розвитком технологій на передній план стали висуватися проблеми власності і володіння електронними інформаційними ресурсами, визначення прав доступу, формулювання вимог до інформаційного ресурсу як товару. Певні інформаційні ресурси в державі стали набувати статусу національних.

Це, в першу чергу, інформаційні ресурси, які містять інформацію з різноманітних аспектів діяльності органів державної влади і місцевого самоврядування, а також юридичних осіб і громадян, що відповідають визначеним вимогам до структури й утримання, та зареєстровані відповідно з регламентованою процедурою. Наприклад, найбільш розвинутою в країні є сфера національних ресурсів науково-технічної інформації. Крім того, для України на даному етапі її розвитку, формування системи управління національними електронними інформаційними ресурсами є стратегічним напрямком і потребує від органів державної влади вирішення проблем, що виникають, з єдиних методологічних позицій.

Аналіз стану електронних інформаційних ресурсів країни визначає множину й інших проблем, які у своїй більшості є загальними для всієї сфери формування і використання інформаційних ресурсів. Серед чинників, що системно впливають на цей комплекс проблем, слід відзначити такі:

- переважно галузевий принцип інформатизації державних органів, що призводить до формування електронних інформаційних ресурсів, орієнтованих, як правило, на задоволення потреб обмеженого кола користувачів;
- відсутність у державних органах та організаціях орієнтації на інформаційне обслуговування громадян;
- неузгодженість і несумісність форматів даних, які зберігаються в різних інформаційних системах, несумісність регламентів і технологій їхнього відновлення, використання різних систем класифікацій і лінгвістичних засобів, що призводить до неоднозначності й суперечливості інформаційних ресурсів різних відомств, неможливості їхнього спільного використання і міжгалузевої взаємодії;
- відсутність сталої системи зберігання та архівування державних електронних документів, документів електронної пошти та електронних

копій паперових документів, а також прийнятих на державному рівні технологій довготривалого зберігання електронних інформаційних ресурсів;

- відсутність єдиних правових норм, які регулюють доступ до державних інформаційних ресурсів, регламентують порядок передачі та використання інформації про діяльність органів державної влади, підприємств і організацій у відкритих мережах і відповідають вимогам інформаційної безпеки.

Ці та інші проблеми в області формування і використання національних інформаційних ресурсів, аналіз їхніх причин свідчать про необхідність корінної зміни пріоритетів у державній політиці в цьому напрямку.

Система національних інформаційних ресурсів - організована за єдиною технологією сукупність національних ресурсів, необхідних для розв'язання завдань соціально-економічного, суспільно-політичного, культурного, духовного розвитку держави (суспільства) та внесених до Національного реєстру електронних інформаційних ресурсів.

Система національних інформаційних ресурсів має відомчі та міжвідомчі ознаки та охоплює інформаційні ресурси:

- органів державної влади і управління, місцевого і регіонального самоврядування;
- державної статистики (державний, обласний, районний рівні);
- архівного, бібліотечного та музейного фондів;
- податкової служби України, правоохоронних і силових структур;
- науково-технічної інформації (створюється у процесі виконання науково-дослідницьких і конструкторських робіт);
- матеріального виробництва, соціальної та фінансової сфер та державного майна і нерухомості.

Окремим видом інформаційних ресурсів, чинне законодавство визначає «інформацію про особу, яка вміщує персональні дані й таємницю особистого життя».

Відповідно до законодавства України прийнято рішення про створення національного реєстру електронних ресурсів - інформаційно-телекомунікаційної системи, призначеної для реєстрації, обліку, накопичення, оброблення і зберігання відомостей про склад, зміст, розміщення, умови доступу до електронних інформаційних ресурсів та задоволення потреб юридичних і фізичних осіб в інформаційних послугах.

До Національного реєстру не включають е-ресурси, які містять відомості, що становлять державну таємницю; інформацію з обмеженим доступом та інформацію, розповсюдження якої заборонене законодавством.

Наступним кроком має стати створення репозитарію електронних ресурсів – інформаційної системи, що забезпечує зосередження в одному місці сучасних електронних інформаційних ресурсів з можливістю надання доступу до них через технічні засоби, у тому числі в інформаційних мережах (як локальних, так і глобальних).

Для забезпечення формування системи національних ресурсів України необхідно розв’язати такі основні завдання:

- забезпечення широкого доступу до ресурсів, у тому числі іноземних, через глобальні інформаційні мережі;
- правове врегулювання суспільних відносин, пов’язаних з формуванням, використанням та захистом національних ресурсів;
- вироблення рекомендацій щодо приведення національних ресурсів до єдиних стандартів на базі новітніх інформаційних технологій, міжнародних стандартів, уніфікованих систем класифікації і кодування інформації;

- створення ефективних національних пошукових, геоінформаційних (комп'ютерні системи, що забезпечують можливість використання, збереження, редагування, аналізу та відображення географічних даних) та навігаційних систем;
- забезпечення розвитку національної освіти, науки, культури через використання новітніх інформаційних технологій;
- залучення до формування системи національних ресурсів недержавних структур;
- створення умов для забезпечення захисту національних ресурсів незалежно від форми власності;
- сприяння наповненню інформаційного ринку національними ресурсами.

Інформаційна інфраструктура. Критична інформаційна інфраструктура держави

Інформаційні ресурси є однією з основних складових ***інформаційної інфраструктури*** (інфраструктури інформаційного простору), яка є системою організаційних структур, що забезпечують функціонування й розвиток інформаційного простору та засобів інформаційної взаємодії.

На думку фахівців, інформаційна інфраструктура є сукупністю:

- інформаційних ресурсів, у т.ч. ЗМІ;
- інформаційних технологій як організованої сукупності систем, засобів, методів і способів, яка забезпечує процеси обробки, зберігання, розвитку, поширення, використання та захисту інформаційних ресурсів;
- інформаційно-телекомунікаційних структур – це комп`ютерні мережі, телекомунікаційні мережі й системи спеціального призначення і загального користування, мережі й канали передачі даних, засоби комутації та управління інформаційними потоками;

- відповідних інституційних складових (обчислювальні центри, інформаційні агенції, оператори та провайдери тощо);
- системи забезпечення, що включає засоби нормативно-правового, економічного забезпечення, стандарти, інструктивні матеріали та документацію, кадрове забезпечення.

Особливий інтерес у контексті інформаційної безпеки держави викликає ***критична інформаційна інфраструктура***, під якою розуміють частину інформаційної інфраструктури, сукупність інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, порушення функціонування яких може призвести до виникнення аварії та/або надзвичайної ситуації, неспроможності держави виконувати свої функції.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» критична інформаційна інфраструктура є сукупністю об'єктів критичної інформаційної інфраструктури, а критично важливими об'єктами інфраструктури (далі - об'єкти критичної інфраструктури) є підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

Під об'єктом критичної інформаційної інфраструктури даний закон розуміє комунікаційну або технологічну систему об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури, а до об'єктів

критичної інфраструктури відносить підприємства, установи та організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об'єктами потенційно небезпечних технологій і виробництв.

Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз затверджуються Кабінетом Міністрів України, а в банківській системі України - Національним банком України.

Відповідно до Директиви Європейської Комісії серед критеріїв визначення елементів критичної інфраструктури ЄС відзначено:

1) масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури завдає значної шкоди);

2) важкість можливих наслідків за такими показниками:

– вплив на населення (число постраждалих, загиблих, осіб, які отримали значні травми, а також чисельність евакуйованого населення);

– економічна шкода (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих);

– екологічна шкода (вплив на населення та навколишнє природне середовище);

– взаємозв'язок з іншими елементами критичної інфраструктури;

– політичний ефект (втрата впевненості в дієздатності влади);

– тривалість впливу (як саме і коли проявлятимуться наслідки, пов'язані зі втратою чи відмовою об'єктів критичної інфраструктури).

Питання для самоконтролю

Що таке інформація, інформаційні відносини, інформаційні ресурси?

Назвіть основні підходи до класифікації інформаційних ресурсів.

Що таке електронні інформаційні ресурси, національні інформаційні ресурси?

Які види інформаційних ресурсів охоплює система національних інформаційних ресурсів?

Що таке інформаційна інфраструктура?

Що називають критичною інформаційною інфраструктурою?

Якими є положення Закону України «Про основні засади забезпечення кібербезпеки України» щодо критичної інформаційної інфраструктури держави?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Боднар І. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки, 2014, № 1. С 68-75.

2. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (29), 2015 р. С.56-61. URL : https://core.ac.uk/download/pdf/47240087.pdf

3. Виговська О., Бєлоусова Н. Інформаційна складова національної безпеки України : кол. монографія / Ін-т міжнар. відносин, Київ. нац. ун-т ім. Тараса Шевченка, Київ. ун-т ім. Бориса Грінченка. Київ : Київ. ун-т ім. Б. Грінченка, 2017. 166 с.

4. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: навч. Посібник. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.

5. Деякі питання діяльності Міністерства культури та інформаційної політики : постанова Кабінету Міністрів України від 16.10.2019 р. № 885 URL : https://zakon.rada.gov.ua/laws/show/885-2019-п#top

6. Єсімов С. С. Шляхи удосконалення нормативно-правового регулювання в сфері інформаційної безпеки. Наукові записки Львівського університету бізнесу та права. 2013. Вип. 11. С. 73-76.

7. Інформаційна безпека держави : навч. посіб. В. М. Рудницький та ін. ; Черкас. держ. технол. ун-т. Харків : ДІСА ПЛЮС, 2018. 358 с.

8. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.

9. Інформаційна безпека. Підручник В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.

10. Кавун С. В., Носов В. В, Манжай О. В. Інформаційна безпека. Навчальний посібник. Харків: Вид. ХНЕУ, 2008. 352 с.

11. Конституція України прийнята 28.06.1996 р. URL : https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

12. Лизанчук В. В. Інформаційна безпека України: теорія і практика : підручник / Львів. нац. ун-т ім. Івана Франка, Львів. шк. журналістики. Львів : ЛНУ ім. Івана Франка, 2017. 725 с.

13. Міжнародна інформаційна безпека: теорія і практика : підруч. для студентів ВНЗ, які навчаються за напрямом підгот. «Міжнародні відносини» та «Міжнародна інформація» / Є. Макаренко та ін. ; Київ. нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин. Київ : Центр вільної преси, 2016. 417 с.

14. Мужанова Т.М. . Інформаційна безпека держави : навчальний посібник. К. : ДУТ. 131 с.

15. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

16. Ніколаєнко Н. О., Комарчук О. О. Засоби масової комунікації як детермінанти гібридної війни : монографія / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2021. 217 с.

17. Панченко О. А. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект : монографія. Київ : КВІЦ, 2020. 331 с.

18. Панченко О.А. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України. Серія: Державне управління. 2019. Випуск 3. 2019. URL : http://77.222.145.174/index.php/governance/article/view/296/297.

19. Перун Т. Загальна характеристика правовідносин у сфері забезпечення інформаційної безпеки в Україні. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2017. № 861. С. 328–332.

20. Питання Міністерства цифрової трансформації : постанова Кабінету Міністрів України від 18.09.2019 р. № 856 URL : https://zakon.rada.gov.ua/laws/show/856-2019-п#Text

21. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 р. URL : https://zakon.rada.gov.ua/laws/show/3475-15#top

22. Про забезпечення участі громадськості у формуванні та реалізації державної політики : постанова Кабінету Міністрів України від 03.11.2010 р. № 996 URL : https://zakon.rada.gov.ua/laws/show/996-2010-п#Text

23. Про затвердження Концепції формування системи національних електронних інформаційних ресурсів : розпорядження Кабінету Міністрів України від 05.05.2003 № 259-р URL : https://zakon.rada.gov.ua/laws/show/259-2003-р#Text

24. Про затвердження Положення про Державний комітет телебачення і радіомовлення України : постанова Кабінету Міністрів України від 13.08.2014 р. № 341 URL : https://zakon.rada.gov.ua/laws/show/341-2014-п#top

25. Про затвердження Положення про Міністерство внутрішніх справ України : постанова Кабінету Міністрів України від 28.10.2015 р. № 878 URL : https://zakon.rada.gov.ua/laws/show/878-2015-п#Text

26. Про захист персональних даних : Закон України від 01.06.2010 р. URL : https://zakon.rada.gov.ua/laws/show/2297-17#Text

27. Про інформацію : закон України від 02.10.1992 р. URL : https://zakon.rada.gov.ua/laws/main/2657-12#Text

28. Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України : Указ Президента України від 22.01.2002 № 63/2002. URL : https://zakon.rada.gov.ua/laws/show/63/2002#Text

29. Про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку : Закон України від 16.12.2021 р. URL : https://zakon.rada.gov.ua/laws/show/1971-IX#Text

30. Про Національну раду України з питань телебачення і радіомовлення : Закон України від 23.09.1997 р. URL : https://zakon.rada.gov.ua/laws/show/538/97-вр#top

31. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 р. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text

32. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. URL : https://zakon.rada.gov.ua/laws/show/537-16#Text

33. Про перелік, кількісний склад і предмети відання комітетів Верховної Ради України дев'ятого скликання : постанова Верховної Ради України від 29.08.2019 № 19-IX URL : https://zakon.rada.gov.ua/laws/show/19-20#top

34. Про рішення Ради національної безпеки і оборони України від 14.05.2021 р. «Про Стратегію кібербезпеки України» : указ Президента України від 26.08.2021 р. URL : https://zakon.rada.gov.ua/laws/show/447/2021#n12

35. Про рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки» : указ Президента

України від 28.12.2021 р. URL : https://zakon.rada.gov.ua/laws/show /685/2021#n14

36. Про рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки» : указ Президента України від 28.12.2021 р. URL : https://zakon.rada.gov.ua/laws/show/ 685/2021#n14

37. Про рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки» : указ Президента України від 28.12.2021 р. URL : https://zakon.rada.gov.ua/laws/show/ 685/2021#n14

38. Про розвідку : Закон України від 17.09.2020 р. URL : https://zakon.rada.gov.ua/laws/show/912-20#top

39. Про Службу безпеки України : Закон України від 25.03.1992 р. URL : https://zakon.rada.gov.ua/laws/show/2229-12#top

40. Рижук О. М. Інформаційна безпека України в умовах глобалізаційних викликів та гібридної війни : монографія / за ред. Бебика В.М. ; Відкр. міжнар. ун-т розвитку людини «Україна». Київ : Університет «Україна», 2019. 177 с.

41. Система забезпечення інформаційної безпеки України. Національна безпека і оборона. 2001. № 1. С. 16-28.

42. Слінько Т. Сучасні загрози інформаційній безпеці країни та шляхи їх подолання. Український часопис конституційного права. 2021. №4. С. 77-84. URL : https://www.constjournal.com/pub/4-2021/suchasni-zahrozy-informatsiyniy-bezpetsi-krainy-shliakhy-ikh-podolannia/

43. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. Підприємство, господарство і право. 2017. №10. С. 182-186. URL : http://pgp-journal.kiev.ua/archive/2017/10/38.pdf

44. https://zakon.rada.gov.ua/laws – законодавство України

45. https://www.kmu.gov.ua/ – Кабінет Міністрів України

46. https://cyberpolice.gov.ua/contacts/ – Кіберполіція Національна поліція України

47. https://ssu.gov.ua/ – Служба безпеки України

48. https://komsvobslova.rada.gov.ua/news/GR_9skl/Polog_GR/74526.html – Комітет Верховної Ради України з питань свободи слова

49. https://thedigital.gov.ua/ – Міністерство цифрової трансформації України

50. https://cip.gov.ua/ua – Державна служба спеціального зв'язку та захисту інформації України

51. https://mkip.gov.ua/ – Міністерство культури та інформаційної політики України

52. http://comin.kmu.gov.ua/ – Державний комітет телебачення і радіомовлення України

53. www.lib.nau.edu.ua/main/ – Науково-технічна бібліотека Національного авіаційного університету