Т Е М А IV.

Інформаційна безпека України

План

1. Поняття, сутність та рівні забезпечення інформаційної безпеки.
2. Державна політика України у сфері інформаційної безпеки.
3. Основні загрози та засоби забезпечення інформаційної безпеки України. Інформаційна війна.
4. Міжнародно-правові засади інформаційної безпеки.

Пит. 1. Поняття, сутність та рівні забезпечення інформаційної безпеки

Питання забезпечення інформаційної безпеки врегульоване ст. 17 Конституції України, ЗУ «Про основи національної безпеки України», Стратегією національною безпеки, затвердженою Указом Президента України від 26.05.2015; Воєнною доктриною України, затвердженою Указом Президента України від 24.09.2015.

Інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Інформаційну безпеку слід розглядати як один з видів національної безпеки, яку, у свою чергу, слід розуміти як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам.

Виходячи зі змісту положень ст. 3 ЗУ «Про основи національної безпеки України» ***об'єктами інформаційної безпеки є:***

- людина і громадянин – їхні конституційні права і свободи:
- суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси:
- держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканість.

Виходячи із зазначеного, в залежності від об’єкта виділяють інформаційну безпеку особи, інформаційну безпеку суспільства та інформаційну безпеку держави.

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

з можливістю вільного одержання, створення й поширення інформації, а також ступінь їхнього захисту від деструктивного інформаційного впливу.

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.*

Відповідно до зазначеного виокремлюють ***три рівня забезпечення інформаційної безпеки:***

- рівень особи (формування раціонального, критичного мислення на основі принципів свободи вибору);
- суспільний рівень (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам);
- державний рівень (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам).**

Передусім, інформаційна безпека досягається реалізацією єдиної державної політики, яка визначає основні напрями діяльності органів державної влади у цій сфері.

Пит. 2. Державна політика України у сфері інформаційної безпеки

Під *державною інформаційною політикою* слід розуміти сукупність напрямів діяльності держави в інформаційній сфері, які ґрунтуються на певній нормативній базі і передбачають, насамперед, посилення інформаційної безпеки держави, суспільства, особи та мають внутрішнє і зовнішнє спрямування.

Основними ***об'єктами державної інформаційної політики*** можна вважати особу, суспільство і державу, а завданнями – забезпечення їх прав та інтересів в інформаційній сфері. Окрім того, до числа об'єктів державної інформаційної політики відносять національну інформаційну сферу з усіма її компонентами (інформаційна інфраструктура, інформаційні ресурси тощо).***

Державна інформаційна політика будується на принципах законності; дотримання балансу життєво важливих інтересів держави, суспільства та особистості; взаємної відповідальності держави, суспільства та особистості за

---

* Петрик В. Сутність інформаційної безпеки держави, суспільства та особи / В. Петрик // Юридичний журнал. – № 5. – 2009. – С. 76.

** Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. : Вид-во НТУ України «КПІ», 2001. – № 4. – С. 43–48.

*** Токар О. Державна інформаційна політика: проблеми визначення концепту / О. Токар // Політичний менеджмент. – № 5. – 2009. – С. 139.

стан безпеки; інтеграції з міжнародними системами забезпечення інформаційної безпеки.[*,**]

Ст. 8 ЗУ «Про основи національної безпеки України» визначено основні ***напрями державної політики*** з питань національної безпеки в інформаційній сфері, зокрема це:

- забезпечення інформаційного суверенітету України;
- удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цін сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- активне залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України;
- забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації та журналістів, заборони цензури, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції, за виконання професійних обов'язків, за критику;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Отже, державна політика в сфері інформаційної безпеки визначає основні напрями діяльності органів державної влади у цій сфері. Зокрема, повноваження **Верховної Ради України** у сфері національної безпеки та її інформаційної складової базуються на положеннях п. 17 ст. 92 Конституції України та характеризуються тим, що основи цієї безпеки визначаються виключно законами України.

Президент України виконує свої повноваження у сфері національної безпеки та її інформаційної складової, керуючись нормами п. 17 ст. 106 Конституції, згідно з якими «здійснює керівництво у сферах національної безпеки і оборони України», та нормами п. 1 ст. 106 Конституції, відповідно до якої забезпечує національну безпеку та її інформаційну складову.

Кабінет Міністрів України відповідно до п.7 ст. 116 Конституції здійснює заходи щодо забезпечення національної безпеки та її інформаційної складової.

Характеризуючи функції державних органів, безпосередньо орієнтованих на вирішення питань інформаційної безпеки, слід звернути увагу на значні зміни у функціях та статусі **Ради національної безпеки і оборони України.** Згідно зі ст. 107 Конституції України РНБО – це координаційний орган з питань національної безпеки і оборони при Президентові України.

***⁎ Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки [Електронний ресурс] / Г. Сащук // Режим доступу : http://journ.univ.kiev.ua/.

Відповідні повноваження конкретизовано в ЗУ «Про Раду національної безпеки і оборони України». Так, до основних ***функцій РНБО*** віднесено (ст. 3):

- внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони;
- координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час;
- координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України.

Для виконання цих завдань РНБО наділена відповідною ***компетенцією***. Серед повноважень цього органу, визначених ст. 4 зазначеного Закону, є кілька ключових, які дозволяють РНБО активно впливати на діяльність органів виконавчої влади та місцевого самоврядування в питаннях, що стосуються сфери національної безпеки. Так, РНБО:

- розробляє та розглядає на своїх засіданнях питання, які відповідно до Конституції та законів України, Стратегії національної безпеки України, Воєнної доктрини України належать до сфери національної безпеки і оборони, та подає пропозиції Президентові України;
- здійснює поточний контроль за діяльністю органів виконавчої влади у сфері національної безпеки і оборони, подає Президентові України відповідні висновки та пропозиції;
- координує і контролює діяльність органів місцевого самоврядування в межах наданих повноважень під час введення воєнного чи надзвичайного стану.

Питання інформаційної безпеки певною мірою вирішуються також у процесі діяльності низки **органів виконавчої влади.** Ці органи можна поділити на ***дві категорії:*** *такі, для яких забезпечення інформаційної безпеки є одним з напрямів діяльності,* і *такі, для яких питання інформаційної безпеки є лише засобом реалізації їх головних функцій*[*].

Органом зі спеціальною компетенцією є **Міністерство інформаційної політики України**, яке діє на підставі Положення «Про Міністерство інформаційної політики України» від 14.01.2015. У 2006 р. створено **Державну службу спеціального зв'язку та захисту інформації України,** яка є державним органом, що 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, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону. Спеціальною компетенцією наділена **кіберполіція**, яка є структурним підрозділом Національної поліції України, що спеціалізується на попередженні, виявленні, припиненні та розкритті

* Кормич Б.А. Інформаційне право : підручник / Б.А. Кормич. – Харків : БУРУН і К., 2011. – С. 142–144.

кримінальних правопорушень, механізми підготовки, вчинення або приховування яких передбачають використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем.

Певні завдання щодо забезпечення інформаційної безпеки виконують підрозділи **Міністерства внутрішніх справ України**. Важливі завдання у сфері забезпечення інформаційної безпеки покладаються на **Службу безпеки України**, яка згідно з нормами ст. 1 ЗУ «Про службу безпеки України» визначається як державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України та, відповідно, інформаційну як її складову.

Працюють у цьому напрямі і різні **дорадчі структури**: Інститут стратегічних досліджень при Президентові України, радники, які запрошуються органами виконавчої влади, та ін.

Пит. 3. Основні загрози та засоби забезпечення інформаційної безпеки України. Інформаційна війна

У правовій доктрині напрацьовано декілька підходів до класифікації загроз інформаційній безпеці. Численність класифікаційних підходів демонструє їх багатоманітність та різнорідність, що вказує на необхідність посилення заходів забезпечення інформаційної безпеки.

Наведемо комплексну ***класифікацію загроз інформаційній безпеці***, згідно з якою вони поділяються на такі групи:

1) за джерелами походження – природного походження, техногенного походження, антропогенного походження;
2) за ступенем гіпотетичної шкоди – загроза та небезпека;
3) за повторюваністю вчинення – повторювані та продовжувані;
4) за сферами походження – екзогенні та ендогенні;
5) за ймовірністю реалізації – вірогідні, неможливі, випадкові;
6) за рівнем детермінізму – закономірні та випадкові;
7) за значенням – допустимі та неприпустимі;
8) за структурою впливу – системні, структурні та елементні;
9) за характером реалізації – реальні, потенційні, здійснені, уявні;
10) за ставленням до них – об’єктивні та суб’єктивні;
11) за об’єктом впливу – ті, що впливають на особу/суспільство/державу.

ЗУ «Про основи національної безпеки України» визначає ***основні загрози*** національним інтересам і національній безпеці України ***в інформаційній сфері,*** до яких належать:

- прояви обмеження свободи слова та доступу до публічної інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;

- розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації.

Однією з найнебезпечніших загроз інформаційній безпеці України є спроби реалізації стратегії інформаційної війни. *Інформаційна війна* – це: 1) дії, вчинені з метою досягнення інформаційної переваги шляхом застосування засобів експлуатації, підриву, знищення, дестабілізації та руйнування інформаційного потенціалу супротивника; 2) застосування засобів захисту власних інформаційних ресурсів і телекомунікаційних систем; 3) дії, вчинені з метою використання інформаційних ресурсів і телекомунікаційних систем іншої сторони, наприклад, електронна війна (інформаційна війна в оборонному і військовому контексті), війна в Інтернеті (інформаційна війна в більш широкому суспільному контексті). Ведення інформаційної війни передбачає обов'язкове використання інформаційної зброї.

Інформаційна зброя – це інформаційні ресурси, стратегічно розроблені або створені для ведення інформаційної війни або для завдання шкоди, збентеження, створення незручностей або будь-яких інших дій зловмисного характеру. Специфіка інформаційної зброї полягає в тому, що об'єктом її застосування може бути будь-який із трьох елементів інформаційної сфери: засоби і лінії зв'язку як матеріальна основа світової інформаційної інфраструктури (до неї належать не лише засоби, поєднані між собою різними каналами зв'язку, але й уся апаратура, призначена для обробки інформації); інформація в чистому вигляді та її потоки; сама людина. Таким чином, застосування інформаційної зброї охоплює: 1) деструктивний вплив на матеріальні об'єкти інформаційної сфери; 2) знищення, спотворення або зміну інформації; 3) цілеспрямований вплив на нервову систему, психіку та свідомість людини. Застосування такої зброї може бути як відкритим в умовах відкритого збройного конфлікту, так і латентним у межах інформаційного протиборства в мирний час.

Види інформаційної зброї:

1) електронні або психічно-електронні засоби, що використовуються незаконними (неконституційними) військовими організаціями, терористичними групами або особами для тимчасової чи перманентної нейтралізації електронних установок або систем;
2) засоби впливу на програмні ресурси електронних засобів контролю з метою їх руйнування або зупинення їх операційних алгоритмів;
3) засоби впливу на процеси передачі інформації з метою їх зупинки або зламу шляхом втручання у середовище розповсюдження сигналу або алгоритм функціонування;
4) засоби поширення дезінформації або створення в інформаційному середовищі віртуальної картини, що повністю або частково змінює уявлення про реальність;

5) засоби дії на людську свідомість та мислення з метою дезорієнтації, втрати сили волі або часткової дестабілізації.*

Види інформаційних війн:

- *кібервійна* – комп'ютерне протистояння у просторі мережі Інтернет, спрямоване на дестабілізацію комп'ютерних систем державних установ, фінансових і ділових центрів, створення безладу та хаосу в житті країни;
- *мережева війна* – форма ведення конфліктів, коли її учасники застосовують мережеві стратегії та технології, пристосовані до сучасної інформаційної доби. Учасниками таких воєн можуть бути терористи, кримінальні угруповання, громадські організації та соціальні рухи, які використовують децентралізацію комп'ютерних систем;
- *електронна війна* – використання та управління інформацією з метою набуття переваги над супротивником шляхом збирання тактичної інформації, забезпечення безпеку власних інформаційних ресурсів, поширення неправдивої інформації про ворога і населення, перешкоджання збиранню інформації супротивником;
- *психологічна війна* – сукупність різних форм, методів і засобів впливу на людину з метою зміни в бажаному напрямку її психологічних характеристик, групових норм поведінки, масових настроїв, суспільної свідомості загалом;
- *радіоелектронна боротьба* – сукупність узгоджених за цілями, задачами, місцем і часом заходів і дій військ, спрямованих на здобування інформації про місцезнаходження радіоелектронних засобів, систем управління військами і зброї супротивника, їх знищення всіма видами зброї, а також радіоелектронне пригнічення сигналів передачі інформації.*

Основні ***шляхи вирішення проблеми інформаційної безпеки*** такі:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;
- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
- розгортання та розвиток Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Державне забезпечення інформаційної безпеки включає:

---

* Кормич Б.А. Інформаційне право : підручник / Б.А. Кормич. – Харків : БУРУН і К., 2011. – С. 150–152.

* Чудінова Н.В., Грицюк Ю.І. Інформаційна безпека України та види джерел загроз і небезпек / Н.В. Чудінова, Ю.І. Грицюк // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами : матер. наук.-практ. конф. (14 грудня 2011 р., м. Львів). – Львів : Львівський ДУВС. – 2011. – С. 250.

- інформування (надання суб'єктам необхідної для функціонування та життєдіяльності достовірної інформації);
- інформатизацію як цілеспрямовану діяльність держави (створення політичних, економічних, технічних та інших умов для інформаційного розвитку суб'єктів, розвитку державного інформаційного ресурсу та оптимізації обміну інформацією);
- унормування поведінки суб'єктів в інформаційній сфері (правова регламентація сфери інформаційних відносин);
- боротьбу з правопорушеннями в інформаційній сфері.

Діяльність із забезпечення інформаційної безпеки складається з таких стадій:

- моніторинг інформаційної сфери (аналіз факторів впливу на інформаційну сферу, виявлення серед них загроз);
- ранжування загроз (встановлення пріоритетності загроз);
- профілактика і попередження негативного впливу загроз;
- безпосередня протидія загрозам.

Засобами забезпечення інформаційної безпеки виступають:

- правова регламентація відносин в інформаційній сфері;
- контрольно-наглядова діяльність;
- інженерно-технічне забезпечення;
- матеріально-технічне забезпечення.

За суб'єктами ***забезпечення інформаційної безпеки поділяється на:***

- державне забезпечення (діяльність державних організацій, спрямована на забезпечення інформаційної безпеки);
- недержавне забезпечення (діяльність громадських організацій та індивідів, спрямована на забезпечення інформаційної безпеки);
- міжнародне забезпечення (сприяння міжнародному співробітництву в галузі інформації, гарантування інформаційного суверенітету держави; сприяння задоволенню інформаційних потреб громадян за кордоном).*

Таким чином, забезпечення інформаційної безпеки покладається не тільки на державу та безпосередньо органи державної влади, але й на міжнародну спільноту та міжнародні організації.

Пит. 4. Міжнародно-правові засади інформаційної безпеки

Кількісне зростання та урізноманітнення інформаційних загроз, а також дедалі більше загострення проблеми кібертероризму вказують на необхідність протидії небезпечним чинникам в інформаційній сфері не тільки на внутрішньодержавному рівні, але й на рівні міжнародному. Забезпечення інформаційної безпеки на міжнародному рівні є складовою предмету регулювання міжнародного інформаційного права. Сучасний етап розвитку

* Тихомиров О.О. Класифікація забезпечення інформаційної безпеки / О.О. Тихомиров // Вісник Запорізького національного університету. – Серія : Юридичні науки. – № 1. – 2011. – С. 166–167.

міжнародного права характеризується формуванням нових галузей, однією з яких є міжнародне інформаційне право світової інформаційної цивілізації.

Міжнародне інформаційне право – це комплексна галузь міжнародного публічного права, що являє собою сукупність правових норм, спрямованих на врегулювання міжнародних відносини в інформаційній сфері.

Комплексний характер міжнародного інформаційного права пояснюється тим, що до його складу входять правові норми та інститути базових і суміжних галузей міжнародного права, об'єднані загальним предметом правового регулювання – міжнародними інформаційними правовідносинами.[**]

У структурі міжнародного інформаційного права пропонують виділяти два ***основні інститути***, до складу яких входять міжнародно-правові норми, спрямовані на врегулювання: 1) *безпосередньо інформаційних відносин*, пов'язаних з внутрішнім інформаційним змістом – «контентом»; 2) *інформаційно-інфраструктурних відносин*, що забезпечують обіг інформаційних ресурсів, інфокомунікацію. Поряд з цим окрему групу утворюють *охоронні та забезпечувальні міжнародно-правові норми, покликані підтримати кібер-стабільність і кібер-мир*[*].

Звертаючись до питання джерел міжнародного інформаційного права, слід зазначити, що, за експертними оцінками, на міжнародному рівні укладено близько 100 міждержавних угод (глобальних, універсальних, регіональних та субрегіональних), спрямованих на врегулювання міжнародних правовідносин в інформаційній сфері. Так, до основних джерел міжнародного інформаційного права відносять: Статут ООН, Загальну декларацію прав людини 1948 р., Міжнародний пакт про громадянські і політичні права 1966 р., Міжнародний пакт про економічні, соціальні та культурні права 1966 р., Конвенцію Ради Європи про захист прав людини і основоположних свобод 1950 р., Європейську культурну конвенцію 1954 р., Міжнародну конвенцію про використання радіомовлення в інтересах миру 1936 р., Європейську конвенцію про транскордонне телебачення 1989 р. тощо. Вказані міжнародні договори ратифіковані Україною та, відповідно, становлять частину національного законодавства нашої держави.

Водночас слід зазначити, що питання забезпечення інформаційної безпеки врегульовані на недостатньому рівні. Так, на міжнародному рівні правові питання боротьби з кібертероризмом вперше було порушено лише у 1990 році, а правові проблеми інформаційної війни та регулювання застосування інформаційної зброї до 1999 року були предметом лише наукових дискусій. Починаючи з 1999 року означене питання стає предметом обговорення на кожній сесії Генеральної Асамблеї ООН, в результаті чого Першим комітетом з питань роззброєння та міжнародної безпеки було прийнято низку резолюцій

[**] Пазюк А. Питання міжнародного інформаційного права: предмет, завдання та принципи / А. Пазюк // Український часопис міжнародного права. – № 1. – 2013. – С. 46–49.

[*] Пазюк А. Питання міжнародного інформаційного права: предмет, завдання та принципи / А. Пазюк // Український часопис міжнародного права. – № 1. – 2013. – С. 46–49.

«Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки».

На сьогоднішній день найбільш значним міжнародно-правовим актом, що регулює питання інформаційної безпеки, є прийнята в межах Ради Європи у 2001 році та ратифікована Україною 2005 року Конвенція про кіберзлочинність. Нормами вказаної конвенції визначаються заходи, які мають здійснюватися на національному та міжнародному рівнях у процесі боротьби з кіберзлочинністю.