

**Тихомиров Олександр Олександрович,**  
*доцент кафедри інформаційної безпеки*  
*держави Національної академії Служби*  
*Безпеки України, доктор юридичних наук,*  
*доцент*

## **СУЧАСНЕ РОЗУМІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ВИМІРИ ТА РІВНІ ЗАБЕЗПЕЧЕННЯ**

Інформаційна еволюція людства й глибина його інтеграції з інформаційними технологіями вносить корективи в парадигму інформаційної безпеки. Інформаційна безпека поступово набуває значення сутнісної основи нормального життя в глобальному інформаційному суспільстві, стаючи своєрідним елементом його культури, базисом подальшого розвитку, особливим об'єктом для права.

На необхідність суттєвих змін у мисленні, світогляді, культурі людини в інформаційному суспільстві, або ж інформаційних трансформаціях картини світу, і, відповідно, розумінні безпеки, дедалі частіше звертають увагу українські вчені. Зокрема, О.В. Прудникова у своїх роботах пропонує філософський образ «людини інформаційної», культура якої є «найважливішим засобом відтворення світової культурної спільноти, створення світового інформаційного простору» [1], подібно «особистості майбутнього» в футурології Е. Тофлера (хвильова концепція). О.П. Дзьобань та Є.М. Мануйлов наголошують на одній з функцій інформаційної культури – «захист від інформаційного стресу, який багато в чому породжується дисбалансом між зростаючим потоком інформації і здатністю суб'єкта (людини, суспільства) до її обробки», а також відзначають безпосередню залежність культурних і безпекових проблем інформаційного суспільства: «...рівень інформаційної культури суб'єкта прямо пропорційний рівню інформаційної безпеки і, причому, що вище рівень інформаційної культури – то менше загроз останньої (тобто то вище рівень інформаційної безпеки) [2].

Водночас, формування уявлень і, далі, концепцій інформаційної безпеки у значній мірі залежить від осмисленості родового явища «безпека». Безпека є складним соціальним феноменом і може мати безліч пояснень, залежних від того чи іншого контексту, або тієї чи іншої галузі діяльності (науки), приміром:

- психологи визначають її як відчуття, сприйняття і переживання необхідності у захисті життєво важливих потреб і інтересів людини;
- юристи (правники) – як систему встановлених законом правових гарантій захищеності особи і суспільства, забезпечення їх нормальної життєдіяльності, прав і свобод;
- філософи – як стан, тенденції розвитку і умови життєдіяльності соціуму та його структур, за яких забезпечується збереження їх якісної визначеності та оптимальне співвідношення свободи і необхідності;

– політологи – як властивість (якість) системи і результат діяльності ряду систем і органів держави, а також сам процес діяльності, спрямованої на досягнення поставлених завдань щодо забезпечення захищеності особи, суспільства, держави.

Тому в сучасних умовах інформаційного розвитку інформаційна безпека набуває комплексного характеру і стає фундаментом існування глобального інформаційного суспільства. Її розуміння має поєднувати соціальні, технологічні, індивідуальні аспекти, включаючи відображення здатності усвідомлювати і задовольняти потреби в необхідній для життєдіяльності (функціонування) інформації. У межах такої соціотехнологічної (соціотехнічної) парадигми [3], серед змістових складових інформаційної безпеки сьогодні достатньо чітко проглядаються:

1) технологічна, яка визначається технічними, технологічними можливостями суб'єктів в інформаційній сфері та є рушійною силою інформаційних трансформацій;

2) правова, як упорядкованість, організованість суспільних інформаційних відносин, що зокрема охоплює нормування, організацію, управління різноманітними інформаційними процесами;

3) медіа, як комплексне відображення впливів суб'єкта (зокрема людини) на інформацію і інформації на суб'єкта в глобальному інформаційному просторі.

Ці три майже традиційні складові інформаційної безпеки на новій стадії інформатизації суспільного життя, яку називають інтелектуалізацією [4] (як в контексті розвитку ІТ, так і власне самої людини) мають логічно доповнюватися когнітивною складовою. Сучасна інформаційно залежна людина поступово перестає бути суто «споживачем інформації», а стає відповідальним користувачем і автором контенту в глобальному інформаційному просторі. Такі зміни зумовлюють розвиток аналітичних здібностей, які є фактичним виразом когнітивного аспекту інформаційної безпеки, зокрема як формування і задоволення потреби в необхідних для певної діяльності (насамперед, прийняття рішень) обсягах інформації та методах її інтерпретації. Як і в інших випадках цю нову складову інформаційної безпеки необхідно розглядати у зв'язку з життєдіяльністю певного суб'єкта, що зумовлює й відповідні напрями забезпечення.

Таким чином, сьогодні інформаційна безпека це складна характеристика певної соціальної системи чи підсистеми, зокрема людини, що відображає здатність до нормальної життєдіяльності (функціонування) й розвитку в певних умовах інформаційного середовища.

Як вже згадувалося, інформаційна безпека не розглядається безвідносно суб'єкта. У значній мірі вона буде результатами діяльності суб'єкта, про безпеку якого йдеться, та, водночас, тими умовами функціонування, що створюються цією діяльністю, а також здатностями до захисту і забезпечення стабільності, які набуваються і розвиваються в процесі цієї діяльності. Тобто, поєднання зазначених змістових складових інформаційної безпеки є універсальним і може розглядатися в різних масштабах (на різних рівнях) – людини, суспільства, держави, окремої організації.

Деталізація за кожною зі складових інформаційної безпеки можлива на різних рівнях – загальних умов, захисних механізмів, індивідуальних можливостей та спроможностей, наприклад таким чином.

#### *1. Технологічна складова:*

##### 1) загальні умови:

- розвиток технологічної бази інформаційного простору;
- впровадження новітніх інформаційних (цифрових) технологій;

##### 2) захисні механізми:

- захист інформації (технічний, програмний, криптографічний);
- забезпечення надійності і достатності систем обробки інформації;

##### 3) індивідуальні можливості й спроможності:

- доступність Інтернету та інформаційних ресурсів;
- забезпеченість сучасними засобами обробки інформації;
- цифрова грамотність.

#### *2. Правова складова:*

##### 1) загальні умови:

- законність і правопорядок в інформаційній сфері;
- упорядкованість важливих видів інформаційної діяльності;
- визнання і юридична визначеність інформаційних прав;
- формування правових засад створення і впровадження нових інформаційних технологій;

##### 2) захисні механізми:

- заборони і юридична відповідальність у сфері інформаційних правовідносин;
- порядок захисту певних категорій інформації, зокрема інформації з обмеженим доступом;
- порядок використання спеціальних засобів отримання інформації;
- окремі механізми захисту і відновлення інформаційних прав;

##### 3) індивідуальні можливості і спроможності:

- правова культура і правосвідомість, інформаційно-правова культура;
- здатності адекватного сприйняття правової інформації;
- орієнтованість на захист власних інформаційних прав.

#### *3. Медіа складова:*

##### 1) загальні умови:

- доступність, багатоманітність, альтернативність медіа та свобода слова;
- популяризація національного інформаційного продукту;
- збереження національної ідентичності і національної культури;
- позитивний імідж суспільства і держави на міжнародній арені;

##### 2) захисні механізми:

- державне регулювання і контроль у сфері медіа;
- захист від маніпуляцій і дезінформації;
- обмеження щодо змісту інформації;
- заходи інформаційної гігієни;

3) індивідуальні можливості і спроможності:

- сформованість інформаційних потреб та культура інформаційних обмінів;
- здатності критичного ставлення до інформації та її джерел;
- медіаграмотність.

Наведений розподіл і деталізація є умовними і лише певною мірою моделюють компонентний склад інформаційної безпеки в межах комплексної парадигми, що також слугує відображенням системи сучасних напрямів і пріоритетів забезпечення інформаційної безпеки.

Описана вище інтеграція діяльнісного та соціотехнічного підходів у розумінні інформаційної безпеки, по-перше, орієнтує на ідеї взаємодії і взаємозалежності людини та інформаційних процесів сьогодні та в перспективі, а по-друге, дає змогу охопити основні наявні напрями визначення інформаційної безпеки, зокрема як управління загрозами, як системи захисних заходів, як захищеності, як умов функціонування (життєдіяльності) та здатностей суб'єктів в інформаційному середовищі, оскільки всі вони інтерпретуються через ті чи інші змістові компоненти діяльності.

#### **Список використаних джерел**

1. Пруднікова О.В. Інформаційна культура: концептуальні засади та світоглядний сенс: монографія. Харків: Право. 2015. 352 с.
2. Дзьобань О.П., Мануйлов Є.М. Інформаційна безпека в контексті інформаційної культури. *Інформація і право*. 2017. № 1(20). С. 74–81.
3. Тихомиров О.О. Інформаційна безпека: соціотехнічна парадигма. *Інформаційна безпека людини, суспільства, держави*. 2014. №1. С. 13–20.
4. Беляков К.І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення : монографія. Київ : КВІЦ, 2008. С. 37–38.

**Бразалук Максиміліан Юрійович,**  
*провідний фахівець відділення соціально-гуманітарної роботи та національно-патріотичного виховання відділу соціально-гуманітарної роботи Національної академії внутрішніх справ*

### **ВПЛИВ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ НА МОРАЛЬНО-ПСИХОЛОГІЧНИЙ СТАН ВІЙСЬКОВОСЛУЖБОВЦІВ ТА ЦИВІЛЬНИХ ОСІБ У КІБЕРПРОСТОРИ**

Складні військово-політичні процеси, з якими щодня стикається наша країна та громадяни, породжують велику кількість проблем, як-то: демографічні, економічні, соціальні, криміногенні, правові, культурні, інформаційні тощо. У своїй сукупності вони утворюють цілу низку викликів як для держави, так і для