ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

# ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРАВООХОРОННИМИ СТРУКТУРАМИ УКРАЇНИ ТА ЗАКЛАДАМИ ВИЩОЇ ОСВІТИ ЗІ СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ

Збірник наукових статей за матеріалами доповідей учасників Всеукраїнської науково-практичної конференції

21 грудня 2018 р.

Львів 2018

УДК 004 П 78

*Рекомендовано до друку Вченою радою Львівського державного університету внутрішніх справ (протокол № 5 від 26.12.2018)*



**П 78** Проблеми застосування інформаційних технологій правоохоронними структурами України та закладами вищої освіти зі специфічними умовами навчання : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції 21 грудня 2018 року / упорядник Т. В. Магеровська / – Львів: ЛьвДУВС, 2018. – 281 с.

У збірнику вміщено наукові статті за матеріалами доповідей учасників Всеукраїнської науково-практичної конференції «Проблеми застосування інформаційних технологій правоохоронними структурами України та закладами вищої освіти зі специфічними умовами навчання», що проводилася 21 грудня 2018 року у Львівському державному університеті внутрішніх справ.

*Опубліковано в авторській редакції*

УДК 004 © Львівський державний університет внутрішніх справ, 2018

# ОСОБЛИВОСТІ ВИЗНАЧЕННЯ СКЛАДОВИХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

***Ткачук Тарас Юрієвич,***

*заступник завідувача кафедри Навчально-наукового інституту інформаційної безпеки Національної академії СБУ, кандидат юридичних наук, доцент*

***Шишко Валерій Валерійович,***

*доцент кафедри теорії та історії держави і права, конституційного та міжнародного права, Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент*

***Хитра Олександра Леонтіївна,***

*доцент кафедри адміністративного права та адміністративного процесу Львівського державного університету внутрішніх справ, кандидат юридичних наук*

Не зважаючи на те, що Конституція України з моменту свого затвердження відносить забезпечення інформаційної безпеки до найважливіших функцій держави [1], нормативне визначення інформаційної безпеки є відносно новим. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» передбачав, що інформаційна безпека – це «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається завдання 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» [2].

Таке визначення, як бачимо, не дає змоги дійти чіткого висновку щодо сутності складових інформаційної безпеки, так само, як і

низка опосередкованих визначень, які розглядають інформаційну безпеку у контексті більш загального поняття – національної безпеки або ж торкаються її окремих аспектів, на кшталт інформаційної безпеки телекомунікаційних мереж [3].

На методологічному рівні предметна сфера інформаційної безпеки є єдиною, структурованою за завданнями та предметом дослідження, збалансованою за терміносистемою. Її системоутворювальним чинником виступають, безумовно, інформація та інформаційні процеси. Утім, для виокремлення складових інформаційної безпеки на доктринальному рівні використовується досить широкий спектр критеріїв, що зумовлює диференціацію підходів до розуміння системного змісту поняття «інформаційна безпека».

Якщо звернутися до зарубіжних наукових джерел, можна переконатись, що найбільш популярною є точка зору, відповідно до якої складовими інформаційної безпеки визнаються цілісність, доступність та конфіденційність інформації [4; 5]. Під цілісністю інформації розуміють її властивість не бути модифікованою неавторизованим користувачем і/або процесом, тобто, зберігатись у стані, визначеному її створювачем та законним володільцем, в т.ч. й достовірність інформації як її відповідність дійсності в аспекті адекватності відображення.

Конфіденційність – це властивість інформації бути недоступною користувачам, які не мають на це права. Ця властивість пов’язана з розмежуванням інформації за режимом доступу.

Доступність інформації полягає в тому, що уповноважений користувач може використовувати її відповідно до правил, встановлених політикою безпеки, не очікуючи більше заданого проміжку часу, тобто це властивість інформації перебувати у необхідному користувачеві вигляді та місці в той час, коли вона йому необхідна.

Справді, належний стан вищезгаданих властивостей є важливим для забезпечення безпеки інформації. Крім того, завдяки забезпеченню безпеки інформації формується нова її властивість – безпечність, котра також є важливою для інформаційної безпеки. Остання ж, окрім власне безпеки інформації, містить й

інші складові. Так, в окремих випадках заподіяння шкоди належному стану властивостей інформації становить лише один з видів протиправних наслідків. Шкода завдається й іншим елементам інформаційної сфери, до яких, окрім інформації, належать також інформаційні системи (суб'єкти й інфраструктура) та інформаційні відносини. Отже, безпека інформації має розглядатися як частина більш масштабного цілого.

Відповідно, науковці як близького зарубіжжя, так і вітчизняні дослідники приділяють значну увагу питанням інформаційно-психологічної та державно-ідеологічної складової інформаційної безпеки, існування яких зумовлюється поділом інформаційної сфери на інформаційно-технічну та інформаційно-психологічну [6, с. 62; 7]. На підставі критерію функціональності вони пропонують також визнавати складовими інформаційної безпеки її аспекти: соціальний; нормативно-правовий; економічний; фінансовий; військовий; екологічний; програмно-технічний та ін. [8].

На думку Б. Кормича, інформаційна безпека має суб'єктно-об'єктний склад, відтак з точки зору критерію основного об'єкта складовими інформаційної безпеки є інформаційна безпека особи, інформаційна безпека суспільства та інформаційна безпека держави. Крім того, держава, людина та суспільство одночасно виступають і в якості суб'єктів інформаційної безпеки, своїми діями здійснюючи захист важливої для них інформації та інформаційних процесів. Зокрема, до сфери інформаційної безпеки держави віднесені конкретні дії щодо забезпечення безпечних умов існуючих інформаційних процесів та забезпечення безпечного розвитку таких процесів у майбутньому, що охоплює регулювання питань захисту самої інформації, захисту інформаційної інфраструктури держави, захисту інформаційного ринку та створення безпечних умов розвитку інформаційних процесів [9, с.30].

Підкреслюючи за результатами комплексного аналізу системність інформаційної безпеки, О.Тихомиров веде мову передусім про «структурні складові забезпечення інформаційної безпеки» та виокремлює їх за різними критеріями, зокрема: за сферами сус-

пільного життя (забезпечення інформаційної безпеки в економічній, політичній, воєнній, науково-технологічній, екологічній, соціальній та інших сферах); за об'єктами національної безпеки (забезпечення інформаційної безпеки особи, суспільства та держави); за сучасними аспектами розуміння інформаційної безпеки (забезпечення інформаційно-психологічної безпеки, забезпечення інформаційної безпеки у сфері прав і свобод людини та забезпечення інформаційно-технічної, в т.ч. кібернетичної безпеки); за основними видами інформаційної діяльності (забезпечення законних можливостей створення, збирання, одержання та використання інформації, законного порядку поширення інформації, належного зберігання інформації, охорона та захист інформації, створення і розвиток інформаційних ресурсів тощо); за формами державного забезпечення інформаційної безпеки (забезпечення якісного інформування, процесів інформатизації; правова регламентація сфери інформаційних відносин; боротьба з правопорушеннями в інформаційній сфері); за напрямами пізнавального процесу в галузі забезпечення інформаційної безпеки (професійна освіта, наукові дослідження, інформаційно-просвітницька діяльність тощо); залежно від елементів змісту діяльності із забезпечення інформаційної безпеки (за об'єктами забезпечення інформаційної безпеки: розвиток і вдосконалення інформаційно-телекомунікаційної інфраструктури, недопущення доведення її до критичного рівня; забезпечення належного використання національних інформаційних ресурсів (захист ресурсів від несанкціонованого втручання, їх інноваційне оновлення, впровадження новітніх технологій створення, оброблення та поширення інформації, формування відкритих інформаційних ресурсів і забезпечення доступу до них громадян); захист інформації (забезпечення конфіденційності, цілісності та доступності тощо); захист свідомості суб'єктів від деструктивного інформаційного впливу (створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей); за суб'єктами забезпечення інформаційної безпеки: міжнародне забезпечення (міжнародне співробітництво в галузі забезпечення інформаційної безпеки, гарантування інформаційного суверенітету держави, сприяння задоволенню інформаційних потреб громадян за

кордоном); державне забезпечення (діяльність державних організацій, спрямована на забезпечення інформаційної безпеки); недержавне забезпечення (діяльність громадських і недержавних комерційних організацій та окремих громадян, спрямована на сприяння державному забезпеченню інформаційної безпеки); за характером предмета діяльності із забезпечення інформаційної безпеки: протидія негативним інформаційним процесам і явищам; сприяння посиленню позитивних інформаційних процесів; сприяння трансформації нейтральних інформаційних процесів у позитивні; за складовими механізму протидії загрозам інформаційній безпеці: моніторинг інформаційної сфери; ранжування загроз; профілактика й попередження негативного впливу загроз; нейтралізація загроз; за характером здійснення державного впливу: безпосереднє створення необхідних умов життєдіяльності суб'єктів в інформаційній сфері; опосередкований вплив шляхом підвищення інформаційного потенціалу суб'єктів і сприяння їх самоорганізації; за засобами забезпечення інформаційної безпеки: правове забезпечення (правова регламентація відносин в інформаційній сфері; контрольно-наглядова діяльність, ліцензування, сертифікації, експертизи тощо); техніко-технологічне забезпечення; залежно від особливостей забезпечення доступу до інформації (за правовим режимом доступу до інформації; за заходами із захисту секретної інформації тощо) [9, с. 31; 10, с. 67].

Проводячи проміжний висновок відзначимо, що вся інформаційна сфера в наш час включає дві основні складові, які, своєю чергою, визначають основні складові інформаційної безпеки держави:

- технічна (штучно створене людиною середовище техніки і технологій);
- психологічна (природній світ з його емоціями).

Джерело: розроблено авторами

Принципові відмінності між визначеними складовими інформаційної безпеки та зміст інформаційно-психологічної складової схематично зображено на рис. 1.

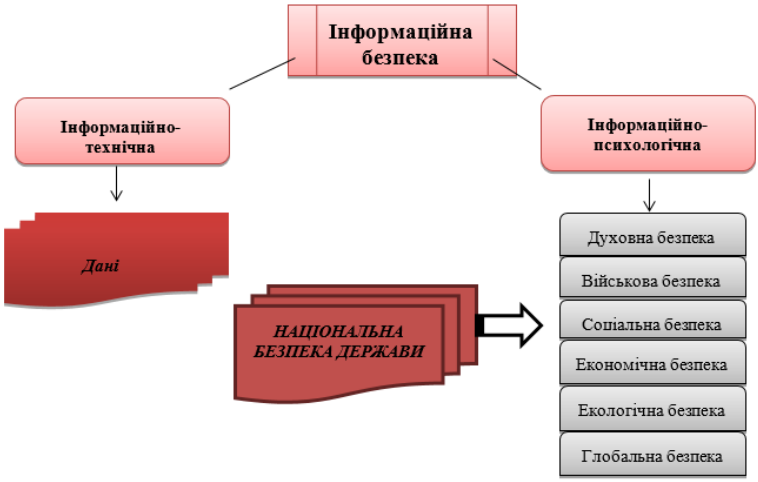


*Рис. 1. Складові інформаційної безпеки*


1. Конституція України від 28.06.1996 року. URL: zakon5.rada.gov.ua/laws /show/254k/96-вр.
2. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 року. URL: zakon5.rada.gov.ua/laws/show/537-16.
3. Про телекомунікації: Закон України від 18.11.2003 року. URL: zakon2.rada.gov.ua/laws/show/1280-15.
4. Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri. An Introduction to Information Security: [Online tool]. Available at. URL: https://doi.org/10.6028/NIST.SP.800-12r1.
5. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec): [Online tool]. Available at. URL: www.cnss.gov/Assets/pdf/nstissi_4011.pdf.
6. Баришполец В.А. Информационно-психологическая безопасность: основные положения/ В.Баришполец //Информационные технологии. – 2013. – №2, том 5. С. 62
7. Уханова Н.С. Інформаційно-психологічна безпека особистості, суспільства та держави. URL: ippi.org.ua/ukhanova-ns-

informatsiino-psikhologichna-bezpekaosobistosti-suspilstva-ta-derzhavi

8. Жатканбаева А. Е. Функциональные компоненты информационной безопасности / А. Жатканбаева// Право и государство. 2013. № 4 (61). С.74.
9. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: [монографія]/ Б.Кормич. – Одеса: Юридична література, 2003. С.28-32.
10. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави: [монографія] / О. Тихомиров; заг. ред. Р. А. Калюжний. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. С.67.